

普通高校本科计算机专业特色教材精选·网络与通信
计算机网络安全学习辅导与实验指南
沈鑫剡 叶寒锋 刘鹏 景丽 编著
清华大学出版社

普通高校本科计算机专业特色教材精选·网络与通信

计算机网络安全学习辅导与实验指南

沈鑫剡　叶寒锋　编著

清华大学出版社
北京

内 容 简 介

本书是《计算机网络安全》(沈鑫剡编著,清华大学出版社出版)的配套辅导教材,也是CCNA安全课程理想的学习辅导和实验指南。每一章由三部分组成:知识要点、例题解析和实验。知识要点部分给出了教材中对应章的知识脉络,重点、难点问题的理解和分析方法。例题解析部分分为自测题、简答题和综合题。自测题用于自我评判对教材内容的理解程度;简答题和综合题使读者进一步理解计算机网络安全的基本概念、方法和技术,掌握解题思路,培养分析、解决问题的能力。实验部分是本书的一大特色,以Cisco Packet Tracer软件为实验平台,针对每一章内容设计了大量帮助读者理解、掌握教材内容的实验,同时也设计了大量旨在帮助读者掌握CCNA安全课程内容的实验。

本书适合作为大专院校计算机专业学生"计算机网络安全"课程的参考书和实验指南,也可作为参加CCNA安全课程学习和用Cisco网络设备进行复杂安全网络设计的工程技术人员的参考书。

图书在版编目(CIP)数据

计算机网络安全学习辅导与实验指南/沈鑫剡,叶寒锋编著.—北京:清华大学出版社,2012.4
(普通高校本科计算机专业特色教材精选·网络与通信)
ISBN 978-7-302-28165-8

Ⅰ.①计…　Ⅱ.①沈…②叶…　Ⅲ.①计算机网络—安全技术—高等学校—教学参考资料
Ⅳ.①TP393.08

中国版本图书馆CIP数据核字(2012)第034046号

责任编辑:袁勤勇　顾　冰
封面设计:
责任校对:胡伟民
责任印制:

出版发行:清华大学出版社
网　　址:http://www.tup.com.cn,http://www.wqbook.com
地　　址:北京清华大学学研大厦A座　　**邮　　编**:100084
社 总 机:010-62770175　　**邮　　购**:010-62786544
投稿与读者服务:010-62776969,c-service@tup.tsinghua.edu.cn
质量反馈:010-62772015,zhiliang@tup.tsinghua.edu.cn
印 刷 者:
装 订 者:
经　　销:全国新华书店
开　　本:185mm×260mm　　**印　　张**:23.5　　**字　　数**:590千字
版　　次:2012年4月第1版　　**印　　次**:2012年4月第1次印刷
印　　数:1～　000
定　　价:　.00元

产品编号:043197-01

本书特色

本书作为《计算机网络安全》配套的学习辅导和实验指南，也是 CCNA 安全课程理想的学习辅导和实验指南。

本书详细介绍 Cisco Packet Tracer 软件实验平台设计、配置和调试各种类型安全网络的方法和步骤，培养学生运用 Cisco 网络设备设计复杂安全网络的能力。

对教材中的难点进行更深入的讨论，理清教材内容的知识结构，给出完整理解教材内容的方法和思路。通过大量的例题解析帮助学生更好地理解教材内容，掌握解题思路，培养分析、解决问题的能力。

出版说明

INTRODUCTION

在我国高等教育逐步实现大众化后，越来越多的高等学校将会面向国民经济发展的第一线，为行业、企业培养各级各类高级应用型专门人才。为此，教育部已经启动了“高等学校教学质量和教学改革工程”，强调要以信息技术为手段，深化教学改革和人才培养模式改革。如何根据社会的实际需要，根据各行各业的具体人才需求，培养具有特色显著的人才，是我们共同面临的重大问题。具体地说，培养具有一定专业特色和特定能力强的计算机专业应用型人才是计算机教育要解决的问题。

为了适应21世纪人才培养的需要，培养具有特色的计算机人才，急需一批适合各种人才培养特点的计算机专业教材。目前，一些高校在计算机专业教学和教材改革方面已经做了大量工作，许多教师在计算机专业教学和科研方面已经积累了许多宝贵经验。将他们的教研成果转化为教材的形式，向全国其他学校推广，对于深化我国高等学校的教学改革是一件十分有意义的事情。

清华大学出版社在经过大量调查研究的基础上，决定组织出版一套“普通高校本科计算机专业特色教材精选”。本套教材是针对当前高等教育改革的新形势，以社会对人才的需求为导向，主要以培养应用型计算机人才为目标，立足课程改革和教材创新，广泛吸纳全国各地的高等院校计算机优秀教师参与编写，从中精选出版确实反映计算机专业教学方向的特色教材，供普通高等院校计算机专业学生使用。

本套教材具有以下特点：

1. 编写目的明确

本套教材是在深入研究各地各学校办学特色的基础上，面向普通高校的计算机专业学生编写的。学生通过本套教材，主要学习计算机科学与技术专业的基本理论和基本知识，接受利用计算机解决实际问题的基本训练，培养研究和开发计算机系统，特别是应用系统的基本能力。

2. 理论知识与实践训练相结合

根据计算机学科的三个学科形态及其关系，本套教材力求突出学科的理论与实践紧密结合的特征，结合实例讲解理论，使理论来源于实践，又进一步指导实践。学生通过实践深化对理论的理解，更重要的是使学生学会理论方法的实际运用。在编写教材时突出实用性，并做到通俗易懂，易教易学，使学生不仅知其然，知其所以然，还要会其如何然。

3. 注意培养学生的动手能力

每种教材都增加了能力训练部分的内容，学生通过学习和练习，能比较熟练地应用计算机知识解决实际问题。既注重培养学生分析问题的能力，也注重培养学生解决问题的能力，以适应新经济时代对人才的需要，满足就业要求。

4. 注重教材的立体化配套

大多数教材都将陆续配套教师用课件、习题及其解答提示，学生上机实验指导等辅助教学资源，有些教材还提供能用于网上下载的文件，以方便教学。

由于各地区各学校的培养目标、教学要求和办学特色均有所不同，所以对特色教学的理解也不尽一致，我们恳切希望大家在使用教材的过程中，及时地给我们提出批评和改进意见，以便我们做好教材的修订改版工作，使其日趋完善。

我们相信经过大家的共同努力，这套教材一定能成为特色鲜明、质量上乘的优秀教材。同时，我们也希望通过本套教材的编写出版，为"高等学校教学质量和教学改革工程"作出贡献。

清华大学出版社

前 言

PREFACE

本书是《计算机网络安全》(沈鑫剡编著,清华大学出版社出版)的配套辅导教材。每一章由三部分组成:知识要点、例题解析和实验。知识要点部分,一是对学生学习过程中碰到的难点进行更深入的讨论;二是理清教材内容的知识结构,给出完整理解教材内容的方法和思路;三是精确描述与网络安全相关的各种技术、概念的本质含义和相互之间区别。大量的例题解析,一是能够帮助学生更好地理解教材内容,掌握解题思路,培养分析、解决问题的能力;二是许多例题都是典型应用的案例,使学生能够将教材内容和实际安全网络设计有机结合,解决学生学以致用的问题;三是通过给出综合运用教材内容进行复杂安全网络分析、设计的详细步骤,为学生树立完整的网络安全知识结构,了解网络安全技术的本质,掌握各种类型安全网络的设计方法和思路。本书最大的特点是实验,基于Cisco Packet Tracer软件,一是针对教材的每一章内容设计了大量的实验,这些实验一部分是教材中的案例和实例的具体实现,用于验证教材内容,帮助学生更好地理解、掌握教材内容,另一部分是实际问题的解决方案,给出用Cisco网络设备设计各种类型安全网络的方法和步骤;二是针对CCNA安全课程内容设计了大量实验,用于帮助读者更好地理解、掌握CCNA安全课程内容。

Cisco Packet Tracer软件的人机界面非常接近实际设备的配置过程,除了连接线缆等物理动作外,学生通过Cisco Packet Tracer软件完成实验与通过实际Cisco网络设备完成实验几乎没有差别,通过Cisco Packet Tracer软件,学生完全可以完成复杂的安全网络的设计、配置和验证过程。更为难得的是,Cisco Packet Tracer软件可以模拟IP分组端到端传输过程中交换机、路由器等网络设备处理IP分组的每一个步骤,显示各个阶段应用层报文、传输层报文、IP分组、封装IP分组的链路层帧的结构、内容和首部中每一个字段的值,使得学生可以直观了解IP分组的端到端传输过程及IP分组端到端传输过程中各层PDU的细节和变换过程。

“计算机网络安全”课程的宗旨是培养学生解决信息存储、传输和处

理过程中面临的安全问题的能力，是一门实验性很强的课程。但目前有的教材只是给学生罗列了大量有关网络安全的概念和术语，提供的实验仅仅是让学生掌握一些扫描和加密软件的使用方法，并不能实现培养学生具有各种类型安全网络的分析和设计能力的教学目标。究其原因，无法提供设计、配置和调试各种类型安全网络的实验环境是导致教学内容落后的重要因素。因此，实现“计算机网络安全”课程的教学目标需要从两个方面着手：一是需要一本提供完整、系统的网络安全理论，深入讨论当前主流网络安全技术，在具体网络环境下讨论运用网络安全技术设计安全网络的方法和过程的教材；二是需要提供一个能够完成各种类型安全网络设计、配置和调试过程的实验环境和一本给出运用教材提供的理论和技术设计、配置和调试各种类型的安全网络的步骤和方法的实验指导书。Cisco Packet Tracer 软件实验平台就是一个能够完成各种类型安全网络设计、配置和调试过程的实验环境，本书提供了在 Cisco Packet Tracer 软件实验平台上运用教材提供的理论和技术设计、配置和调试各种规模的安全网络的步骤和方法。《计算机网络安全》和本书相得益彰，学生用教材提供的安全网络设计原理和技术指导实验，反过来又通过实验来加深理解教材内容，课堂教学和实验形成良性互动。

本书由解放军理工大学工程兵工程学院计算机应用教研室的沈鑫剡和吉林大学研究生叶寒锋共同编写，由沈鑫剡定稿。限于作者的水平，错误和不足之处在所难免，殷切希望使用本书的老师和学生批评指正，也殷切希望读者能够就本书内容和叙述方式提出宝贵建议和意见，以便进一步完善本书内容。作者 E-mail 地址为 shenxinshan@163.com。

编者

2011 年 10 月

目录

CONTENTS

第1章 概 述

CHAPTER

1.1 知识要点

1.1.1 黑客攻击对象和攻击手段

黑客对网络的攻击可以分为对主机系统攻击和对通信系统的攻击。

1. 主机系统攻击手段

(1) 在主机系统运行恶意代码。

通过下属手段,在主机系统运行恶意代码。

- 手工植入恶意代码并激活。
- 在下载的网络资源中植入病毒。
- 利用主机系统漏洞上传并激活病毒。

(2) 利用主机系统漏洞非法登录。

通过下属手段,非法登录主机系统。

- 利用主机系统漏洞非法建立管理员账户,利用非法建立的管理员账户登录主机系统。
- 利用激活的木马程序非法访问主机系统资源。
- 利用主机系统错误开放的服务,如共享服务、远程调用服务非法访问主机系统资源。

(3) 穷举攻击。

- 猜测主机系统登录口令。
- 利用字典破解主机系统登录口令。

2. 通信系统攻击手段

(1) 信息嗅探攻击。

信息嗅探攻击是指非法窃取经过网络传输的信息,但不影响信息正常传输过程的攻击行为。

(2) 信息截获攻击。

信息截获攻击是指截获经过网络传输的信息,使信息无法继续正常传输的攻击行为。截获信息是篡改信息,实施重放攻击的前提。

(3) 重放攻击。

重放攻击是指黑客截获信息,延迟一段时间后,转发或反复转发截获的信息的攻击行为。重放攻击一般不对截获的信息进行处理。

(4) 拒绝服务攻击。

拒绝服务攻击是指通过消耗掉服务器处理资源、转发结点处理资源、物理链路带宽,使网络不能提供正常服务的攻击行为。

(5) 非法接入。

非法接入是指黑客将终端非法接入内部网络的行为,如未经授权建立和无线局域网接入点之间的关联,通过盗用的用户名和口令接入启动 802.1X 接入控制功能的交换机端口等。非法接入是对网络实施攻击的第一步。

(6) 诱骗攻击。

黑客通过接入伪造的 DHCP 服务器,使终端获取错误的网络配置信息,导致终端对网络资源的访问过程出现问题。更严重的是,黑客通过伪造的 DHCP 服务器和伪造的 DNS 服务器将一些著名网站的域名和黑客伪造的 Web 服务器的 IP 地址绑定在一起,使得用户对著名网站的访问变为对黑客伪造的 Web 服务器的访问。

(7) 路由项欺骗攻击。

通过向路由器发送伪造的路由项,使得路由器错误地将黑客终端作为通往某个网络的传输路径的下一跳,并将所有以该网络中的终端为目的终端的 IP 分组转发给该黑客终端。

3. 被动攻击和主动攻击

网络攻击可以分为被动攻击和主动攻击,被动攻击只是窃取信息,不会影响信息正常的存储、处理和传输过程,信息嗅探攻击是典型的被动攻击。主动攻击篡改已经存在的信息,影响信息正常的传输和处理过程,甚至伪造信息,信息截获攻击、重放攻击、各种欺骗攻击(包括源 IP 地址欺骗攻击、DHCP 欺骗攻击和 DNS 欺骗攻击等)和拒绝服务攻击是典型的主动攻击。主要通过预防,而不是检测来应对被动攻击。主动攻击是网络面临的主要安全问题,应对主动攻击需要各种安全机制(包括信息备份和恢复技术)的有机结合。

1.1.2 信息安全与网络安全

1. 信息安全目标

信息安全目标是保障网络中信息资源的保密性、完整性、可用性、可控制性和不可抵赖性。网络中的信息资源包括存储在主机系统中的信息资源和经过网络传输的信息资源,因此,保障信息资源的完整性包括保障主机系统的完整性。可用性是综合指标,用于评估信息资源提供服务的能力,涉及通信系统、主机系统等多个方面。

2. 信息安全功能

(1) 消除主机系统漏洞。

主机系统漏洞包括操作系统漏洞和应用程序漏洞,它们是导致黑客入侵的主要原因。消除主机系统漏洞是避免黑客入侵的最有效方法,但完全消除主机系统漏洞是不现实的,因此,较长时间段内会是一个反复进行发现漏洞、利用漏洞入侵、修补漏洞的过程。

(2) 避免主机系统植入恶意代码。

主机系统一旦植入恶意代码,将导致信息外泄,破坏信息的保密性;可能使主机系统崩溃,破坏信息的可用性;也可能篡改存储在主机系统中的信息,破坏信息的完整性。主机系统植入恶意代码是信息资源最大的安全隐患。网络是目前传播病毒的主要渠道,因此除了在主机系统安装查杀病毒软件外,必须有效隔断经过网络传播病毒的通道。

(3) 确保经过网络传输的信息的保密性和完整性。

网络应用导致大量信息经过网络传输,必须保证这些经过网络传输的信息的保密性和完整性,因此必须采取有效手段杜绝信息嗅探、信息截获攻击的发生。

(4) 隔断黑客和攻击目标之间的通道。

目前大量利用主机系统漏洞实施的攻击行为都是远程攻击行为,黑客必须经过网络实现和攻击目标之间的信息传输,必须能够鉴别出黑客实施攻击的信息流,并阻断黑客和攻击目标之间的信息流传输通道。

3. 信息安全技术

(1) 加密、报文摘要和鉴别算法。

加密、报文摘要和鉴别算法是信息安全的基础,是保障信息保密性、完整性的有效手段。

(2) 安全操作系统。

安装一个安全操作系统是防御黑客入侵的关键。安全操作系统是指没有漏洞;能够通过用户身份鉴别和授权对用户访问信息资源过程实施有效控制;能够通过制定用户行为规则发现病毒,并对病毒破坏信息资源行为实施反制;能够对主机系统资源实施有效保护的操作系统。

(3) 安全应用程序。

运行安全应用程序也是防御黑客入侵的必要手段。安全应用程序是指没有漏洞;能够通过用户身份鉴别和授权对用户访问信息资源过程实施有效控制的应用程序。

(4) 安全传输机制。

安全传输机制是指保障信息传输过程中的保密性和完整性的机制,包括有效防止黑客实施信息嗅探和信息截获攻击的机制、信息加密和完整性检测机制、信息源端鉴别机制等。

(5) 接入控制机制。

接入控制机制是指保证只有授权终端接入网络,且使得网络只允许传输、接收端只允许接收授权终端发送的信息的机制,包括双向身份鉴别机制、安全参数协商机制和基于用户的接入控制机制等。

(6) 访问控制机制。

访问控制机制保证授权用户只能访问到授权访问的信息,包括只在授权用户使用的终端和授权访问的信息资源所在主机系统之间建立传输通路的机制、只允许授权用户使用的终端和授权访问的信息资源所在主机系统之间传输与完成访问授权访问的信息有关的信息流的机制。

(7) 隔离病毒机制。

隔离病毒机制是指防止病毒传播，隔断病毒网络中传播途径的机制，包括检测出与病毒传播和因为病毒发作引发的攻击行为有关的信息流并予以丢弃的机制、禁止主机系统之间发生与病毒传播相似的信息流传输模式的机制。

4. 网络安全范畴

网络安全是信息安全的重要组成部分，网络安全可以定义为是所有用于保障传输过程中的信息的安全、阻断病毒传播和黑客非法访问途径、应对各种各样网络攻击手段的机制和技术的集合，它不包括信息安全技术中的安全操作系统和安全应用程序的内容。

1.1.3 网络安全内容和体系结构

1. 网络安全内容

(1) 基础理论。

加密算法、报文摘要算法和鉴别算法等。

(2) 接入控制和访问控制机制。

802.11X、802.11i、PPP 和 PPPoE、VPN、防火墙和入侵防御系统等。

(3) 防御远程攻击和阻断病毒传播路径机制。

阻止端口扫描和漏洞探测机制、阻断病毒传播路径机制、端到端安全传输机制和流量管制机制等。

(4) 防御信息嗅探和信息截获攻击机制。

以太网安全机制、安全路由机制、虚拟网络技术、IP Sec 和 TLS 等。

(5) 防御诱骗攻击机制。

信任端口、DNS Sec、HTTPS 和 SET 等。

(6) 网络管理和监测机制。

基于 SNMPv3 的网络管理系统和网络综合监测系统等。

2. 网络安全体系结构

网络安全体系结构如图 1.1 所示，它由两部分组成：一部分是网络安全基础，它所包含的加密、报文摘要算法、数字签名技术、身份鉴别机制和各种安全协议是所有网络安全技术的基础。另一部分是作用于网络每一层的安全技术。

<table>
<tr><td colspan="6">HTTPS、SET、SSL VPN、PGP等</td><td colspan="2">应用层</td></tr>
<tr><td colspan="6">有状态检测、信息流管制等</td><td colspan="2">传输层</td></tr>
<tr><td colspan="6">安全路由协议、IPSec、分组过滤、NAT等</td><td colspan="2">网际层</td></tr>
<tr><td rowspan="2">以太网</td><td>安全端口，接入控制</td><td rowspan="2">无线局域网</td><td>802.11i</td><td rowspan="2">接入网络</td><td>接入控制、VPN、L2TP</td><td>链路层</td><td rowspan="2">网络接口层</td></tr>
<tr><td>电缆、光缆保护，电磁屏蔽</td><td>信号能量控制</td><td>电缆、光缆保护，电磁屏蔽</td><td>物理层</td></tr>
<tr><td colspan="6">加密、报文摘要和数字签名技术
TLS、RADIUS等</td><td colspan="2">网络安全基础</td></tr>
</table>

图 1.1 网络安全体系结构

1.2　例题解析

1.2.1　自测题

1. 选择题

（1）下述________不属于网络面临的安全问题。
A. 病毒　　B. 拒绝服务攻击
C. 非法访问　　D. 网络设备快速更新

（2）下述________不属于引发网络安全问题的原因。
A. 网络原旨是方便通信
B. 大量商务活动在网上展开
C. 网络信息资源已经成为重要的战略资源
D. 网络安全设备发展迅速

（3）下述________无法破坏网络的可用性。
A. 病毒　　B. 拒绝服务攻击　　C. 非法访问　　D. 线缆遭受破坏

（4）下述________和信息保密性无关。
A. 加密解密算法　　B. 终端接入控制　　C. 病毒　　D. 拒绝服务攻击

（5）下述________和信息完整性无关。
A. 加密解密算法　　B. 报文摘要算法　　C. 信息嗅探攻击　　D. 信息截获攻击

（6）下述________和黑客远程入侵主机系统无关。
A. 操作系统漏洞　　B. 应用程序漏洞
C. 黑客和主机系统之间信息传输路径　　D. 主机系统的物理安保措施

（7）下述________和病毒植入主机系统无关。
A. 操作系统漏洞　　B. 配置主机系统网络信息方式
C. 黑客和主机系统之间信息传输路径　　D. 主机系统的物理安保措施

（8）下述________和信息嗅探攻击有关。
A. 操作系统漏洞　　B. 应用程序漏洞
C. 信息传输路径　　D. 主机系统的物理安保措施

（9）下述________和信息截获攻击有关。
A. 操作系统漏洞　　B. 应用程序漏洞
C. 配置主机系统网络信息方式　　D. 主机系统的物理安保措施

（10）下述________和诱骗用户登录伪造的著名网站无关。
A. 篡改 DNS 服务器的资源记录　　B. 伪造 DNS 服务器
C. 配置主机系统网络信息方式　　D. 著名网站的物理安保措施

（11）下述________和阻止信息截获攻击无关。
A. 禁止伪造的 DHCP 服务器接入网络　　B. 鉴别 DNS 资源记录
C. 鉴别路由消息　　D. 用交换机取代集线器

(12) 下述________和阻止信息嗅探攻击无关。

A. 交换机端口静态配置为全双工通信方式

B. 鉴别 DNS 资源记录

C. 交换机端口之间禁止镜像

D. 用交换机取代集线器

(13) 下述________和病毒传播无关。

A. 主机系统之间复制文件　　B. 浏览 Web 主页

C. 阅读邮件　　D. 变换终端接入 Internet 方式

(14) 加密和报文摘要算法一般不能阻止下述________攻击。

A. 信息嗅探　　B. 信息截获　　C. 篡改信息　　D. 重放

(15) 加密和报文摘要算法不能完成下述________操作。

A. 完整性检测　　B. 源端鉴别

C. 数据加密　　D. 阻止伪造的 DHCP 服务器接入网络

(16) 下述________攻击和操作系统漏洞无关。

A. 非法登录主机系统

B. 向主机系统植入病毒

C. 缓冲器溢出

D. 消耗掉主机系统连接网络的链路的带宽

(17) 下述________攻击和通信系统无关。

A. 远程入侵主机系统　　B. 传播病毒

C. 截获信息　　D. 物理破坏主机系统

(18) 下述________和阻止病毒传播无关。

A. 入侵防御系统　　B. 防火墙

C. 接入控制机制　　D. 禁止从光盘引导系统

(19) 下述________和阻止黑客远程入侵主机系统无关。

A. 入侵防御系统　　B. 防火墙

C. 接入控制机制　　D. 禁止读写 U 盘

2. 填空题

(1) 信息安全目标是保证信息的________、________、________、________和________。

(2) ________、________和________是三种分别通过攻击主机系统达到破坏信息的可用性、保密性和完整性目的的攻击行为。其中，________破坏信息的可用性，________破坏信息的保密性，________破坏信息的完整性。

(3) ________、________和________是三种分别通过攻击通信系统达到破坏信息的可用性、保密性和完整性目的的攻击行为，其中，________破坏信息的可用性，________破坏信息的保密性，________破坏信息的完整性。

(4) ________、________和________是三种常见的病毒传播方法。

(5) ________、________和________是三种常用的可以阻止病毒传播的安全机制。

（6）接入控制只允许授权用户使用的终端接入网络，首先需要完成用户的________，以此确定是否授权用户，以后通过该终端发送的信息中必须携带________，以此确定该信息是否由授权用户发送。

（7）完整性检测是________和________的结合，其中________必须具有单向性和抗冲突性的特性。

（8）数字签名必须具有________、________和________特性，其中，________用于确认由签名者本人做出的承诺，________用于确认对特定信息做出的承诺，________保证第三方能够证明签名与签名者之间的关联。

（9）安全路由保证传输路径一不是根据________生成的，二是________。

（10）加密解密算法根据加密密钥和解密密钥是否相同可以分为________和________，________由于加密密钥和解密密钥相同，导致密钥分发比较困难。

（11）网络攻击可以分为________和________两大类，________主要通过加密予以预防，________不是单一安全机制可以应对的，需要集成各种安全机制予以解决。

（12）计算机网络面临的主要威胁有________和________。

3. 名词解释

____入侵防御系统　　____接入控制机制
____信息安全　　____网络安全
____加密解密算法　　____报文摘要算法
____拒绝服务攻击　　____数字签名
____信息嗅探攻击　　____信息截获攻击
____鉴别算法　　____防火墙
____授权　　____访问控制
____病毒　　____蠕虫
____木马　　____证书
____重放攻击　　____非法访问

（a）用于保障网络中信息资源安全的技术、机制和系统的集合。

（b）所有用于保障传输过程中的信息的安全、阻断病毒传播和黑客非法访问途径、应对各种各样网络攻击手段的技术、机制和系统的集合。

（c）两种互逆的改变原有数据内容的算法，改变数据内容的计算过程中需要用到密钥。

（d）一种可以将任何长度报文变成固定长度摘要，且能够保证不能够从摘要反推出原始报文，也不能够根据一个报文推导出另一个摘要相同的不同报文的算法。

（e）一种用于证实用户或终端和某个标识符之间关联的算法。

（f）一种位于网络边界，对网络间进行的数据交换过程实施控制的设备。

（g）一种能够获得流经某条链路，或进入某个主机的信息，并能够对获得的信息是否异常做出判断，并加以干预的设备。

（h）一种能够完成用户授权，且保证只允许授权用户使用的终端接入网络，网络只允许传输、接收端只允许接收授权用户使用的终端发送的信息的机制。

(i) 一段需要寄生在别的程序中的代码,激发后,可以将自己反复插入到其他程序中,并在条件成熟时实施破坏动作。

(j) 一种具备完整程序特性的恶意代码,能够自动传播到其他系统,并具有自动激发功能,因而能够快速传播。

(k) 一种恶意代码,其主要功能在于削弱主机系统的安全性,并盗取主机系统的信息资源。

(l) 一种由权威机构颁发,证明某个标识符与某个公钥之间绑定关系的文件。

(m) 一种通过过度消耗链路或结点资源,使其无法正常提供服务的攻击手段。

(n) 一种只能由唯一的用户或机构对特定报文生成的标识信息,且这种标识信息的唯一性和与特定报文之间的关联可以通过第三方证明。

(o) 未经授权,非法复制经过网络传输的信息的攻击行为,但这种攻击行为一般不会影响信息的正常传输过程。

(p) 通过改变信息传输路径使信息到达非授权接收信息的终端,且使授权接收信息的终端无法接收信息的攻击行为。

(q) 截获信息,延迟一段时间后,转发或反复转发截获的信息的攻击行为。

(r) 获取没有授权获取的信息的行为。

(s) 一种用于确定特定用户网络中信息资源访问权限的过程,完成这个过程后,网络中建立用于保障和限制该用户按照权限访问信息资源所需的控制信息。

(t) 所有用于保证用户只能访问授权访问的信息的技术、机制和系统的集合。

4. 判断题

(1) 只要目的地址正确,分组就不会错误地传输给其他终端。

(2) 只要安装杀毒软件,定时更新病毒特征库,就不可能感染病毒。

(3) 操作系统和应用程序漏洞是蠕虫入侵的主要渠道。

(4) 对称密钥算法的密钥分发很困难。

(5) 不对称密钥算法的密钥分发比较容易。

(6) 任何两个不同报文的报文摘要肯定不同。

(7) 检测病毒是入侵防御系统的主要任务。

(8) 只要操作系统存在漏洞,主机系统就无法避免远程入侵。

(9) 安装病毒查杀软件是应对病毒感染和传播的唯一方法。

(10) 黑客攻击就是利用主机系统漏洞上传并激活病毒。

(11) 访问控制是主机系统的功能。

(12) 加密和报文摘要算法是实现信息保密性和完整性的基础。

(13) 身份鉴别是访问控制的重要功能之一。

(14) 大量攻击不是主机系统能够解决的。

(15) 利用网络实现远程攻击和病毒传播是黑客的主要攻击手段。

(16) 数字签名可以用于身份鉴别。

(17) 网络安全是信息安全的重要组成部分。

1.2.2 自测题答案

1. 选择题答案

(1) D,只有这项不属于网络安全问题。

(2) D,引发网络安全问题的原因：一是网络协议和技术着重于实现通信,忽略安全；二是大量商务活动在网上开展,使得攻击者有利可图；三是网络中的信息资源事关一个单位、甚至一个国家的成败。

(3) C,非法访问一般只窃取信息资源,不破坏网络系统。

(4) D,拒绝服务攻击一般只破坏网络系统的可用性。

(5) C,信息嗅探攻击只是非法窃取信息,无法篡改信息,因此,它破坏的只是信息的保密性。

(6) D,黑客实现远程入侵的前提是发现存在漏洞的主机系统,且建立黑客终端与该主机系统之间的传输路径。D与这两项无关。

(7) B,病毒植入分为本地植入和经过网络远程植入,B项只会影响主机系统信息传输方式,与病毒经过网络远程植入主机系统关系不大。

(8) C,信息嗅探攻击通常指非法复制经过网络传输的信息,且这种复制不会影响信息的正常传输过程。

(9) C,截获信息攻击需要改变信息传输路径,只有C项能够做到这一点。

(10) D,诱骗用户登录伪造的著名网站需要将著名网站的域名和某个伪造成该著名网站的Web服务器的IP地址绑定在一起,D项与这个过程无关。

(11) D,实施信息截获攻击或是给出错误的通往目的终端的传输路径,或是给出错误的目的终端的IP地址(或物理地址),只有D项与阻止这两件事情的发生无关。

(12) B,信息嗅探攻击既要窃取信息,又要不影响信息的正常传输过程,只有B项与破坏这两点无关。

(13) D,终端用何种方式接入Internet与病毒传播没有多大关系。

(14) D,重放攻击无需还原明文、无需篡改信息,只是延迟一段时间后转发,或者反复转发截获的原始报文。

(15) D,加密和报文摘要算法无法阻止伪造的DHCP服务器接入网络。

(16) D,消耗通信系统资源的拒绝服务攻击与主机系统漏洞无关。

(17) D,只有这项攻击不需要经过通信系统传输信息。

(18) D,阻止病毒传播,一是禁止主机系统之间相互复制感染病毒的文件,二是禁止病毒经过网络传播,D项与这两件事情无关。

(19) D,阻止黑客远程入侵主机系统,一是消除主机系统存在的漏洞,二是阻止黑客发现该主机系统的漏洞,三是禁止黑客和该主机系统交换与实施攻击有关的信息。D项与这三件事情无关。

2. 填空题答案

(1) 保密性,完整性,可用性,不可抵赖性,可控制性。

(2) SYN泛洪攻击,木马,篡改Web主页,SYN泛洪攻击,木马,篡改Web主页。

(3) Smurf 攻击,信息嗅探攻击,篡改信息攻击,Smurf 攻击,信息嗅探攻击,篡改信息攻击。

(4) 利用邮件传播,浏览嵌入病毒的主页,利用主机系统漏洞上传病毒。

(5) 防火墙,入侵防御系统,查杀病毒软件。

(6) 身份鉴别,唯一标识授权用户的标识信息。

(7) 加密算法,报文摘要算法,报文摘要算法。

(8) 唯一性,关联性,可证明性,唯一性,关联性,可证明性。

(9) 伪造的路由项,安全的。

(10) 对称加密算法,不对称加密算法,对称加密算法。

(11) 被动攻击,主动攻击,被动攻击,主动攻击。

(12) 非法访问,拒绝服务攻击。

3. 名词解释答案

g 入侵防御系统	h 接入控制机制
a 信息安全	b 网络安全
c 加密解密算法	d 报文摘要算法
m 拒绝服务攻击	n 数字签名
o 信息嗅探攻击	p 信息截获攻击
e 鉴别算法	f 防火墙
s 授权	t 访问控制
i 病毒	j 蠕虫
k 木马	l 证书
q 重放攻击	r 非法访问

4. 判断题答案

(1) 错,有太多的攻击手段可以将一个目的地址正确的分组传输给一个错误的终端。

(2) 错,目前大多数杀毒软件都是基于病毒特征的,通常都是在发现病毒造成的后果后,才会发现病毒,分析病毒,提取病毒特征。

(3) 对,蠕虫通常通过目标主机操作系统和应用程序的漏洞上传到目标主机,并自动激活。

(4) 对,由于对称密钥算法的加密解密密钥相同,必须将密钥限制在授权参与数据加密解密的终端。

(5) 对,由于不对称密钥算法用公钥加密数据,用私钥解密数据,因此公钥的分发比较容易。

(6) 错,肯定存在两个具有相同报文摘要的不同报文,只是报文摘要算法保证根据现有计算能力,无法根据某个报文 P 找出另一个报文 P',$P \neq P'$,但它们的报文摘要相同。

(7) 错,入侵防御系统的主要任务是检测异常信息流,并加以干预。

(8) 错,完成远程入侵,一是主机系统存在漏洞,二是黑客能够通过网络发现该主机系统的漏洞,三是黑客和主机系统之间能够通过网络完成实施攻击所需的信息交换过程。如果能够阻止后两件事情发生,即使某个主机系统存在漏洞,黑客也无法远程入侵该主机

系统。

(9) 错，查杀病毒软件只是一种事后弥补的机制，在网络中隔断病毒传播途径才是事先预防机制。

(10) 错，黑客攻击多种多样，有对主机系统实施的攻击，有对通信系统实施的攻击，利用主机系统漏洞上传并激活病毒只是针对主机系统的其中一种攻击行为。

(11) 错，访问控制的本质是只允许授权用户访问到授权访问的信息，它包括只允许授权用户使用的终端接入网络、只在授权用户使用的终端与存在授权访问的信息资源的主机系统之间建立传输路径、主机系统只允许访问授权访问的信息等控制功能。完成这些控制功能需要综合多种网络安全机制。

(12) 对，加密防止信息外泄，报文摘要和加密能够实现完整性检测。

(13) 对，首先通过身份鉴别确定是否是授权用户。

(14) 对，不但主机系统无法解决对通信系统实施的攻击，大部分对主机系统实施的攻击也需要综合多种网络安全机制才能解决。

(15) 对，网络环境下，黑客对主机系统的攻击和病毒传播都是通过网络实施的。

(16) 对，数字签名有着唯一性和与特定报文之间的关联性，而且这种唯一性和关联性可以被第三方证明，因此可以通过数字签名确定报文发送者的身份。

(17) 对，网络安全只讨论信息安全中与保障信息传输安全、控制信息传输路径、阻断病毒传播和黑客非法访问途径等相关的技术、机制和系统。

1.2.3　简答题解析

1. 简述防止黑客远程入侵主机系统机制。

回答： 一是主机系统及时通过补丁软件消除漏洞；二是主机系统通过授权和身份鉴别对信息资源访问过程进行监控；三是通过接入控制机制禁止非授权用户使用的终端接入网络；四是通过防火墙和入侵防御系统禁止与实施漏洞扫描和利用漏洞实施攻击相关的信息到达主机系统。

2. 简述防止病毒传播机制。

回答： 一是主机系统安装查杀病毒软件；二是通过流量管制限制某种可能与病毒传播相关的信息流的流量，如某个终端单位时间内发送邮件的流量；三是入侵防御系统检测出与病毒传播和因为病毒发作引发的攻击行为有关的信息流，并予以丢弃；四是防火墙访问控制策略尽量禁止主机系统之间发生与病毒传播相似的信息流传输模式；五是对访问的网站的真实性进行鉴别，防止访问到伪造的著名网站提供的嵌入病毒的主页。

3. 简述网络安全功能和相关技术、机制。

回答： 网络安全功能包括保障信息传输过程中的保密性和完整性；保证只有授权终端接入网络且使得网络只允许传输、接收端只允许接收授权终端发送的信息；保证授权用户只能访问到授权访问的信息；防止病毒传播；隔断病毒网络中传播途径等。

相关技术和机制包括恶意代码分析与防御；黑客攻击机制分析与防御；加密和报文摘要算法；鉴别协议和数字签名；一般网络安全技术；无线局域网安全技术；虚拟专用网络设计；防火墙；入侵防御系统；网络管理和监测；应用层安全协议等。

1.3 Cisco Packet Tracer 5.3 使用说明

1.3.1 功能介绍

“计算机网络安全”课程的教学目标是掌握完整、系统的网络安全理论和当前主流网络安全技术，具备用主流网络安全技术解决实际网络安全问题的能力。实现上述教学目标需要提供良好的实验环境，但建设能够完成各种网络安全实验的实验环境的费用是很高的。另外，对于一个初学者而言，实际设计、配置和调试一个安全网络的过程固然重要，掌握各种安全技术的工作原理和各种安全协议之间的相互作用过程更加重要，而一般的实验环境无法让初学者观察、分析各种安全技术和安全协议工作过程中的每一个步骤。

Cisco Packet Tracer 5.3 是 Cisco 为网络初学者提供的一个学习软件，初学者通过 Packet Tracer 可以用 Cisco 网络设备设计、配置和调试一个安全网络，而且可以模拟各种安全技术和安全协议工作过程中的每一个步骤。除了不能实际物理接触外，Packet Tracer 提供了和实际实验环境几乎一样的仿真环境。

1. 安全网络设计、配置和调试过程

根据安全网络设计要求选择 Cisco 网络设备，如路由器、交换机等，用合适的传输媒体将这些网络设备互连在一起，进入设备配置界面对网络设备逐一进行配置，检验安全网络的接入控制和访问控制功能，如果发现问题，通过检查网络拓扑结构、互连网络设备的传输媒体、设备配置、设备建立的控制信息(如访问控制列表、交换机转发表和路由器路由表等)确定问题的起因，并加以解决。

2. 模拟协议操作过程

只有了解网络环境下各种安全协议的工作流程、各种网络安全技术的工作机制及它们之间的相互作用过程，才能掌握完整、系统的网络安全知识。对于初学者，掌握网络设备之间各种安全协议实现过程中相互传输的报文类型、报文格式、报文处理流程对理解安全网络工作原理至关重要。Packet Tracer 模拟操作模式给出了各种安全协议实现过程中每一个步骤涉及的报文类型、报文格式及网络设备处理报文的流程，可以让初学者观察、分析安全协议实现过程中的每一个细节。

3. 验证教材内容

本书的主要特色是在讲述每一种网络安全技术和安全协议前，先构建一个学生能够理解的网络环境，并在该网络环境下详细讨论网络安全技术的工作机制、安全协议的工作流程，而且所提供的网络环境和人们实际应用中所遇到的实际网络十分相似，较好地解决了课程内容和实际应用的衔接问题。在教学过程中，可以用 Packet Tracer 完成教材中每一个网络环境的设计、配置和调试过程，同时可以用 Packet Tracer 模拟操作模式给出安全协议实现过程中的每一个步骤，以及每一个步骤涉及的报文类型、报文格式和报文处理流程，以此验证教材内容，并通过验证过程更进一步加深学生对教材内容的理解，真正做到弄懂弄透。

1.3.2 用户界面

启动 Packet Tracer 5.3 后，出现图 1.2 所示的用户界面。

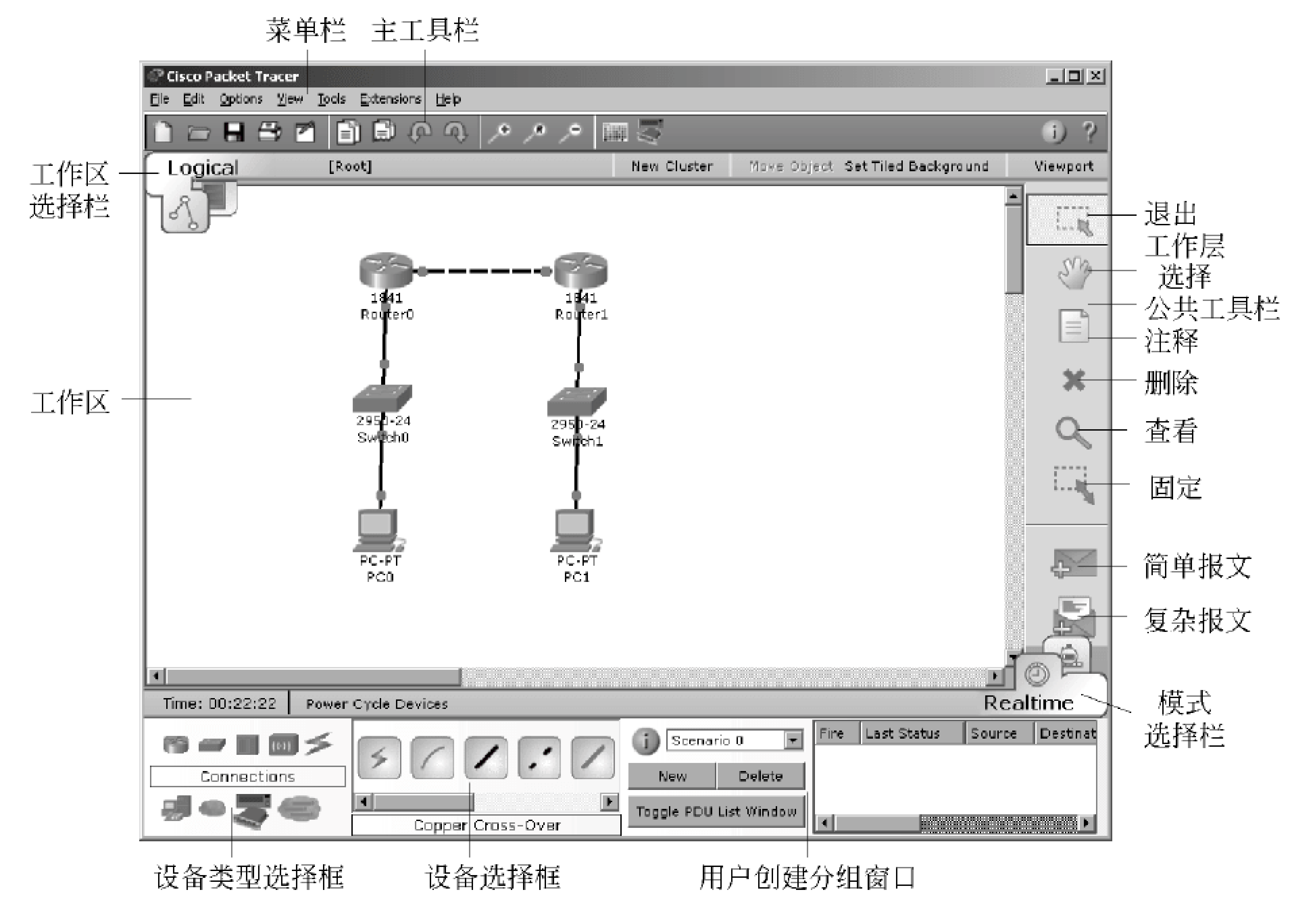


图 1.2 Packet Tracer 5.3 用户界面

菜单栏：提供该软件的 7 个菜单，其中 File(文件)菜单给出工作区新建、打开和存储文件命令。Edit(编辑)菜单给出复制、粘贴和撤销输入命令。Options(选项)菜单给出 Packet Tracer 的一些配置选项。View(视图)菜单给出放大、缩小工作区中某个设备的命令。Tools(工具)菜单给出几个分组处理命令。Extensions(扩展)菜单给出有关 Packet Tracer 扩展功能的子菜单。Help(帮助)菜单给出 Packet Tracer 详细的使用说明，所有初次使用 Packet Tracer 的读者必须详细阅读 Help 菜单中给出的使用说明。

主工具栏：给出 Packet Tracer 的常用命令，这些命令通常包含在各个菜单中。

公共工具栏：给出对工作区中构件进行操作的工具，如添加注释、删除构件和查看构件配置等。

工作区：作为逻辑工作区时，用于设计网络拓扑结构、配置网络设备、检测端到端连通性等。作为物理工作区时，给出城市布局、城市内建筑物布局和建筑物内配线间布局等。

工作区选择栏：可以选择物理工作区和逻辑工作区，物理工作区中可以设置配线间所在建筑物或城市的物理位置，网络设备可以放置在各个配线中间，也可以直接放置在城市中。逻辑工作区中给出各个网络设备之间的连接状况和拓扑结构。可以通过物理工作区和逻辑工作区的结合检测互连网络设备的传输媒体的长度是否符合标准要求，如一旦

互连两个网络设备的双绞线缆长度超过 100m，两个网络设备连接该双绞线缆的端口将自动关闭。

模式选择栏：可以在实时操作模式和模拟操作模式之间选择，实时操作模式可以验证网络任何两个终端之间的连通性；模拟操作模式可以给出分组端到端传输过程中的每一个步骤，以及每一个步骤涉及的报文类型、报文格式和报文处理流程。

设备类型选择框：设计网络时，可以选择多种 Cisco 网络设备，设备类型选择框用于选择网络设备的类型。设备类型选择框中给出的网络设备类型有交换机、路由器、集线器、无线设备、连接线、终端设备和云设备等，云设备用于仿真广域网，如 PSTN、ADSL 接入网等。

设备选择框：用于选择指定类型的网络设备型号，如果在设备类型选择框中选中路由器，可以通过设备选择框选择 Cisco 各种型号的路由器。

用户创建分组窗口：为了检测网络任意两个终端之间的连通性，需要生成并端到端传输分组。为了模拟协议操作过程和分组端到端传输过程中的每一个步骤，也需要生成分组，并启动分组端到端传输过程，用户创建分组窗口就用于用户创建分组并启动分组端到端传输过程。

1.3.3 工作区分类

工作区选择作为物理工作区时，工作区用于给出城市间地理关系、每一个城市内建筑物布局、建筑物内配线间布局等，如图 1.3 所示。当然，也可以直接在城市中某个位置放置配线间和网络设备。New City 按钮用于在物理工作区创建一座新的城市。同样，New Building、New Closet 按钮用于在物理工作区创建一栋新的建筑物和一间新的配线间。一般情况下，在指定城市中创建并放置新的建筑物，在指定建筑物中创建并放置新的配线

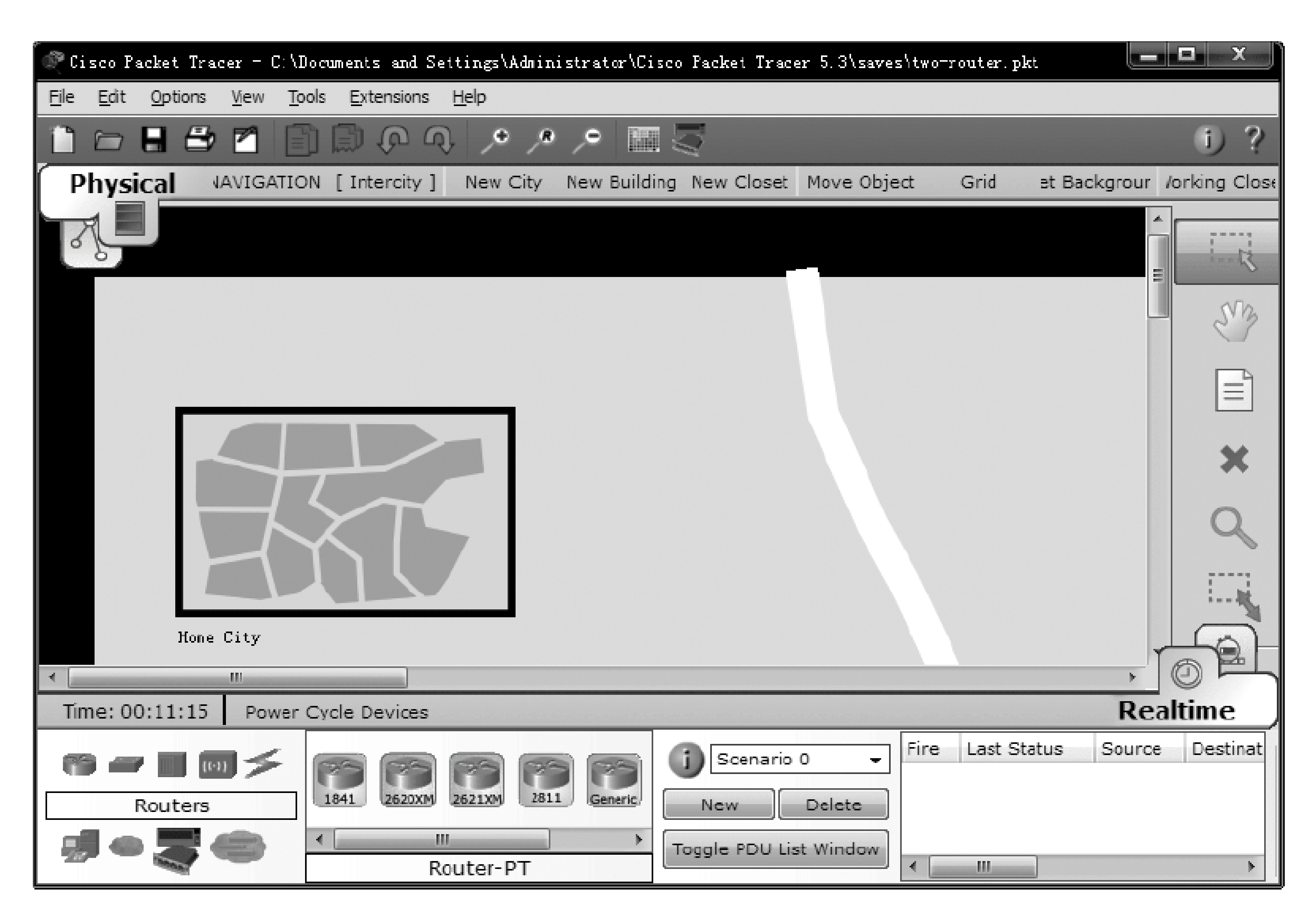


图 1.3 物理工作区

间。逻辑工作区中创建的网络所关联的设备初始时全部放置于本地城市中公司办公楼内的主配线中间，可以通过 Move Object 菜单完成网络设备配线间之间的移动，也可直接将设备移动到城市中，当两个互连的网络设备放置在不同的配线间时，或城市不同位置时，可以计算出互连这两个网络设备的传输媒体的长度。如果启动物理工作区距离和逻辑工作区设备之间的连通性之间的关联，一旦互连两个网络设备之间的传输媒体距离超出标准要求，两个网络设备连接该传输媒体的端口将自动关闭。

1.3.4　操作模式

Packet Tracer 操作模式分为实时操作模式和模拟操作模式。实时操作模式仿真网络实际运行过程，用户可以检查网络设备配置，转发表、路由表等控制信息，通过发送分组检测端到端连通性。模拟操作模式下，用户可以观察、分析分组端到端传输过程中的每一个步骤。图 1.4 是模拟操作模式的用户界面，Event List（事件列表）给出协议报文或分组的逐段传输过程，单击事件列表中的某个报文，可以查看该报文的内容和格式。Scenario（情节）用于设定模拟操作模式需要模拟的过程，如分组的端到端传输过程。Auto Capture/Play 按钮用于启动整个模拟操作过程，按钮下面的滑动条用于控制模拟操作过程的速度，事件列表列出根据情节进行的模拟操作过程所涉及的协议报文或分组的逐段传输过程。Capture/Forward 按钮用于单步推进模拟操作过程。Back 按钮用于回到上一步模拟操作结果。Edit Filters（编辑过滤器）菜单用于选择情节模拟操作过程中涉及的协议。通过单击事件列表中的协议报文或分组可以详细分析协议报文或分组格式，对应段相关网络设备处理该协议报文或分组的流程和结果。因此，模拟操作模式是找出网络不能正常工作的原因的理想工具，同时也是初学者深入了解协议操作过程和网络设备处

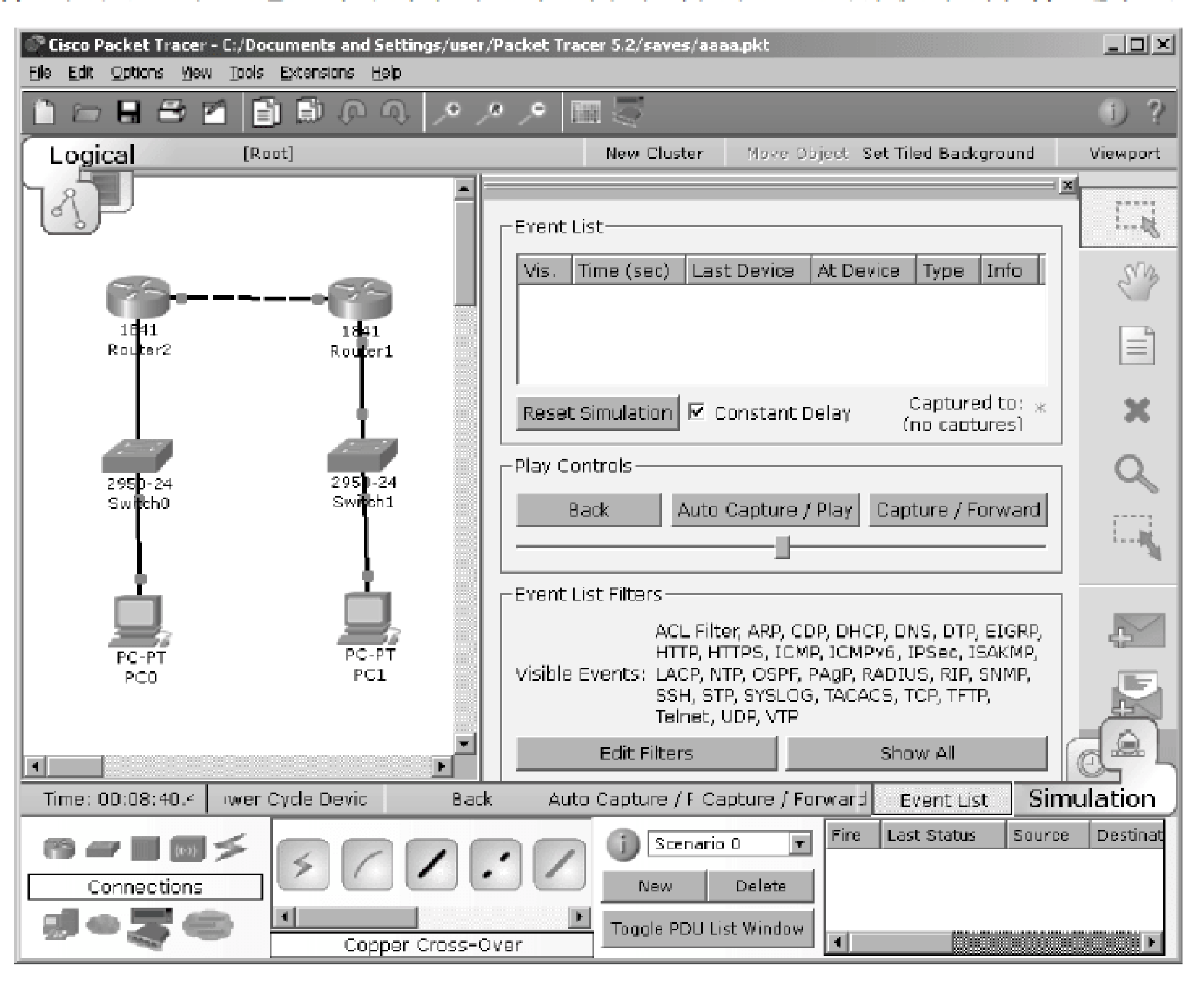


图 1.4　模拟操作模式

理协议报文或分组的流程的理想工具，模拟操作模式是实际网络环境无法提供的学习工具。

1.3.5 设备类型和配置方式

Packet Tracer 提供了设计复杂互连网络可能涉及的网络设备类型，如交换机、路由器、集线器、无线设备、连接线、终端设备和云设备等。其中云设备用于仿真广域网，如PSTN、帧中继等，通过云设备可以设计出由广域网为互连路由器的传输网络的复杂互连网络。

一般在逻辑工作区和实时操作模式下进行网络设计，如果用户需要将某个网络设备放置到工作区中，用户在设备类型选择框中选择特定设备类型，如路由器，然后在设备选择框中选择特定设备型号，如 Cisco 1841 路由器，按住鼠标左键将其拖放到工作区的任意位置，释放鼠标左键。单击网络设备进入网络设备的配置界面，每一个网络设备通常有物理、图形接口和命令行接口(Command Line Interface，CLI)三个配置选项，物理配置选项用于为网络设备选择可选模块，图 1.5 是路由器 1841 的物理配置界面，可以为路由器的两个插槽选择模块。为了将某个模块放入插槽，首先关闭电源，然后选定模块，按住鼠标左键将其拖放到指定插槽，释放鼠标左键。如果需要从某个插槽取走模块，同样也是先关闭电源，然后选定某个插槽模块，按住鼠标左键将其拖放到模块所在位置，释放鼠标左键。插槽和可选模块允许用户根据应用环境扩展网络设备的接口类型和数量。

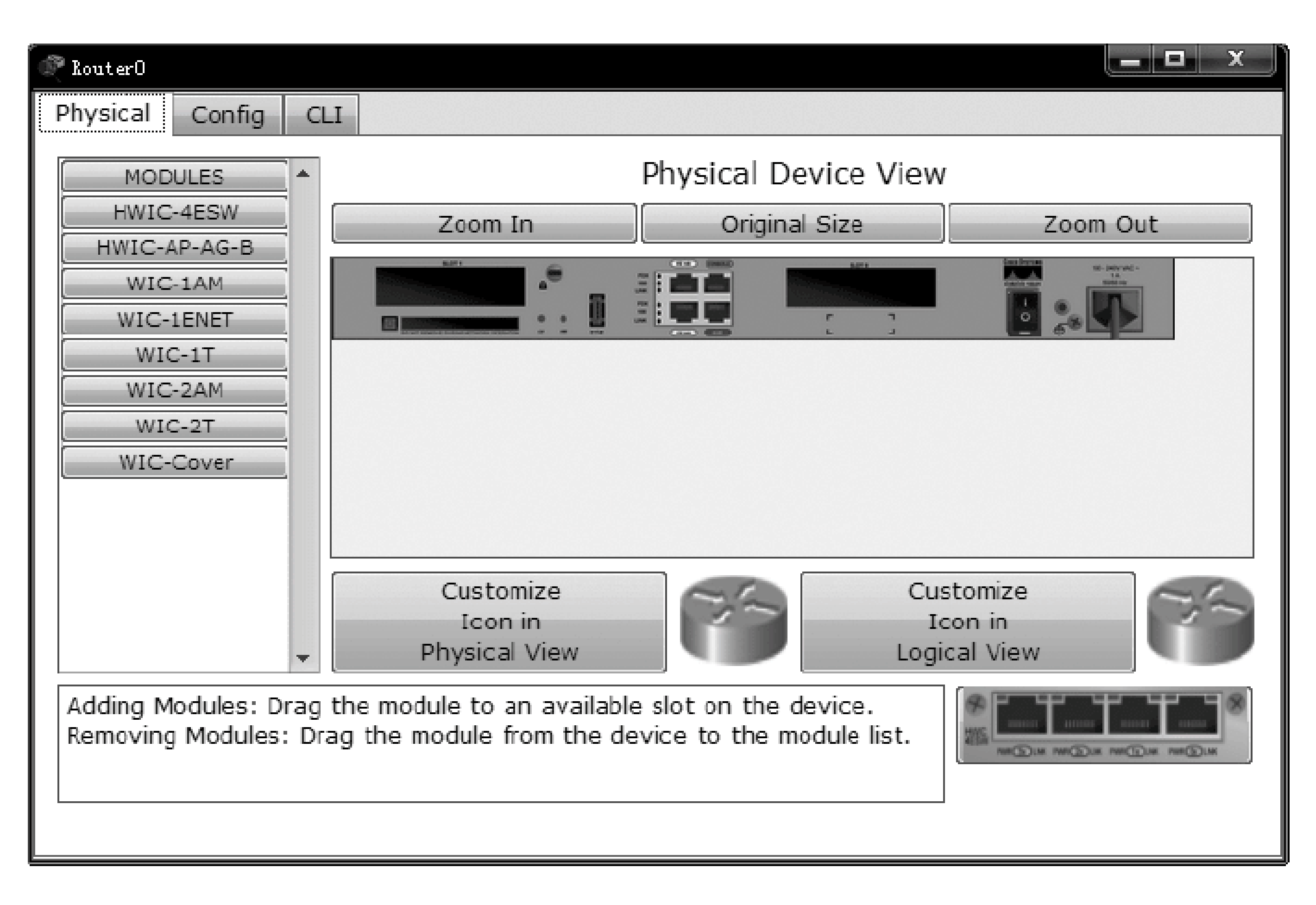


图 1.5 路由器 1841 物理配置界面

图形接口为初学者提供方便、易用的网络设备配置方式，是初学者入门的捷径。图 1.6 是路由器 1841 图形接口的配置界面，初学者很容易通过图形接口配置路由器接口的 IP 地址、子网掩码，配置路由器静态路由项等。图形接口不需要初学者掌握 Cisco 配置命令就能完成一些基本功能的配置，配置过程直观、简单且容易理解。更难得的是，在用图形接口配置网络设备的同时，Packet Tracer 给出完成同样配置过程需要的配置命令序列。通过图形接口提供的基本配置功能，初学者可以完成简单网络的配置，并观察简单

网络的工作原理和协议操作过程,以此验证课程内容。但随着课程内容的深入和复杂安全网络设计,要求读者能够通过命令行接口配置网络设备的一些复杂的功能。因此,一开始,同时用图形接口和命令行接口完成网络设备的配置过程,同时也通过相互比较,进一步加深对 Cisco 配置命令的理解,随着课程学习的深入,强调用命令行接口完成网络设备的配置过程。

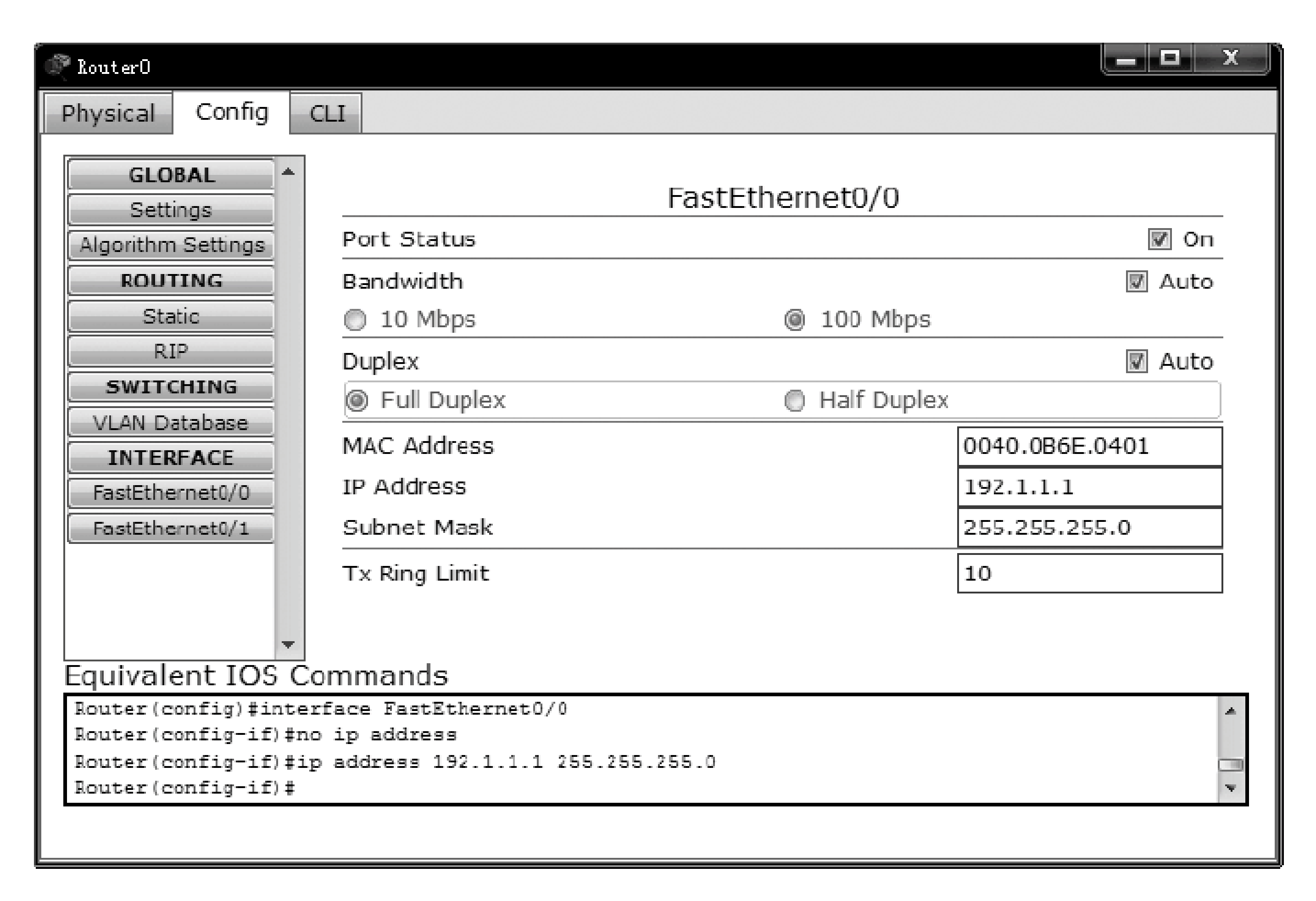


图 1.6　图形接口配置界面

命令行接口提供与实际配置 Cisco 设备完全相同的配置界面和配置过程,因此是读者需要重点掌握的配置方式。掌握这种配置方式的难点在于需要读者掌握 Cisco 配置命令,并会灵活运用这些配置命令,因此,在以后章节中不仅对用到的 Cisco 配置命令进行解释,还对命令的使用方式进行讨论,让学生对 Cisco 配置命令有较为深入的理解。图 1.7 是命令行接口的配置界面。

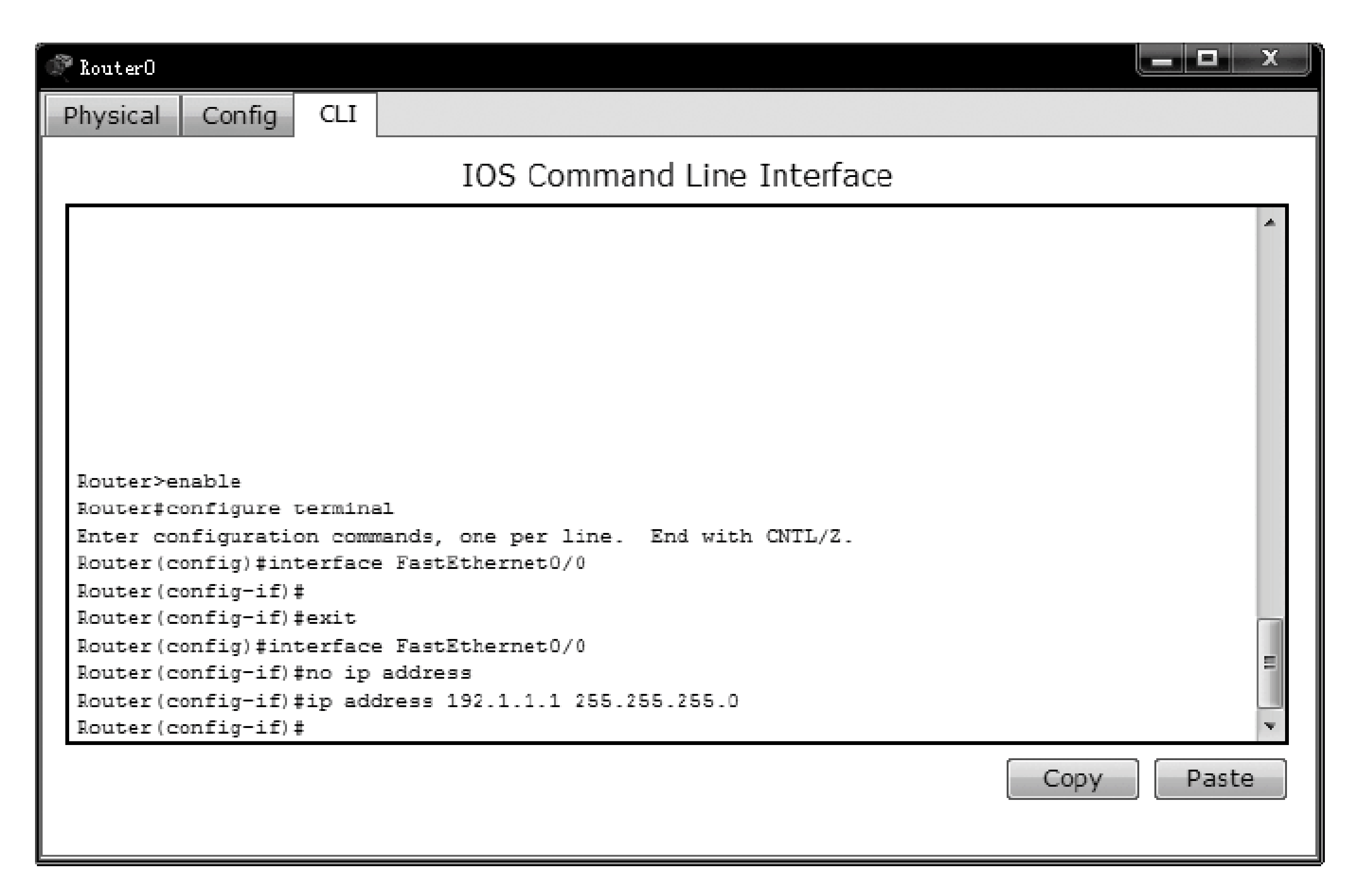


图 1.7　命令行接口配置界面

这里只对 Packet Tracer 5.3 做一些基本介绍,具体通过 Packet Tracer 5.3 完成安全

网络设计、配置和调试的过程与步骤在以后讨论具体网络安全实验时再予以详细讲解。

1.4 实 验

1.4.1 信息嗅探攻击实验

1. 实验内容

(1) 完成互连网络设计。

(2) 验证 IP 分组端到端传输机制。

(3) 完成信息嗅探攻击过程。

2. 网络结构

网络结构如图 1.8 所示。如果交换机和路由器之间插入集线器,用集线器互连交换机、路由器和黑客终端,则黑客终端将嗅探到终端 A 和终端 B 与服务器之间交换的全部 IP 分组。

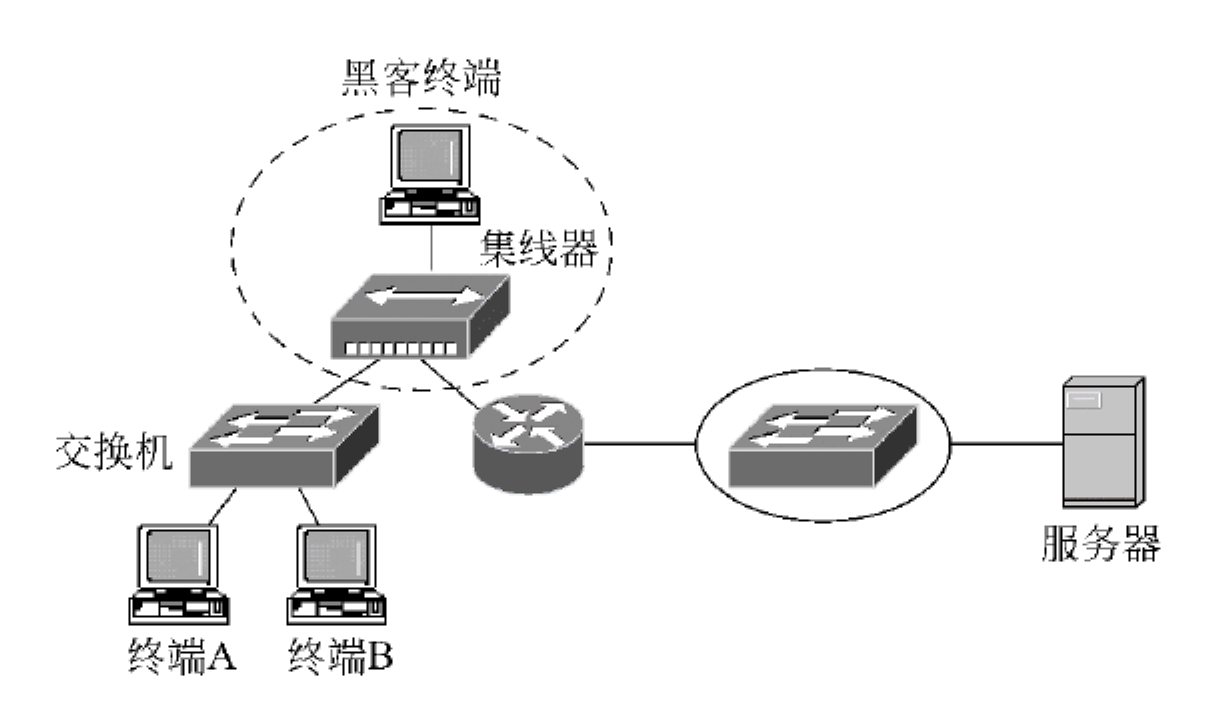


图 1.8 信息嗅探攻击原理

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区按照图 1.8 所示网络结构放置和连接设备,但先用直连双绞线直接连接交换机 Switch1 和路由器 Router0。直连双绞线将一端的发送端口和接收端口与另一端的发送端口和接收端口直接连接。交叉双绞线将一端的发送端口和接收端口与另一端的发送端口和接收端口交叉连接。终端和交换机之间、交换机和路由器之间用直连双绞线连接。放置和连接设备后的逻辑工作区界面如图 1.9 所示。

(2) 为路由器接口配置 IP 地址和子网掩码,接口 FastEthernet0/0 配置 IP 地址和子网掩码 192.1.1.254/24,接口 FastEthernet0/1 配置 IP 地址和子网掩码 192.1.2.254/24,确定这两个接口所连接的网络的网络地址分别为 192.1.1.0/24 和 192.1.2.0/24。连接在这两个网络上的终端必须配置与所连接的网络的网络地址一致的 IP 地址和子网掩码,并以路由器连接该网络的接口的 IP 地址为默认网关地址。路由器接口 FastEthernet0/0 的配置界面如图 1.10 所示。由于终端 PC0、PC1 连接在路由器接口 FastEthernet0/0 所连接的网络上,这两个终端配置的 IP 地址和子网掩码必须与网络地

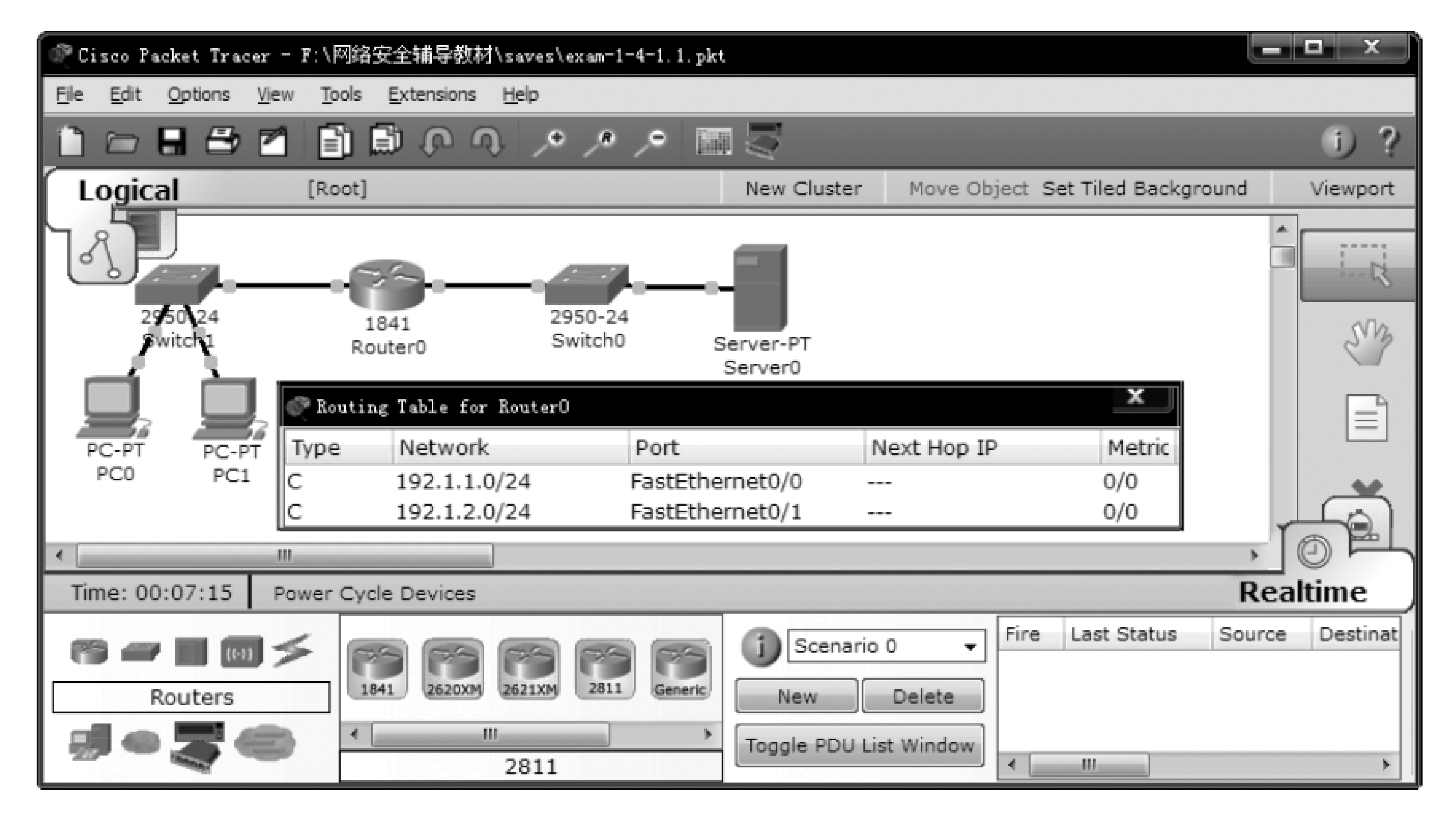


图 1.9　正常互连网络结构及路由表

址 192.1.1.0/24 一致，并以 IP 地址 192.1.1.254 为默认网关地址。PC0 配置 IP 地址和子网掩码的界面如图 1.11 所示，配置默认网关地址的界面如图 1.12 所示。单击 FastEthernet 按钮，弹出 PC0 以太网接口 IP 地址和子网掩码配置界面。单击 Settings 按钮，弹出 PC0 默认网关地址配置界面。

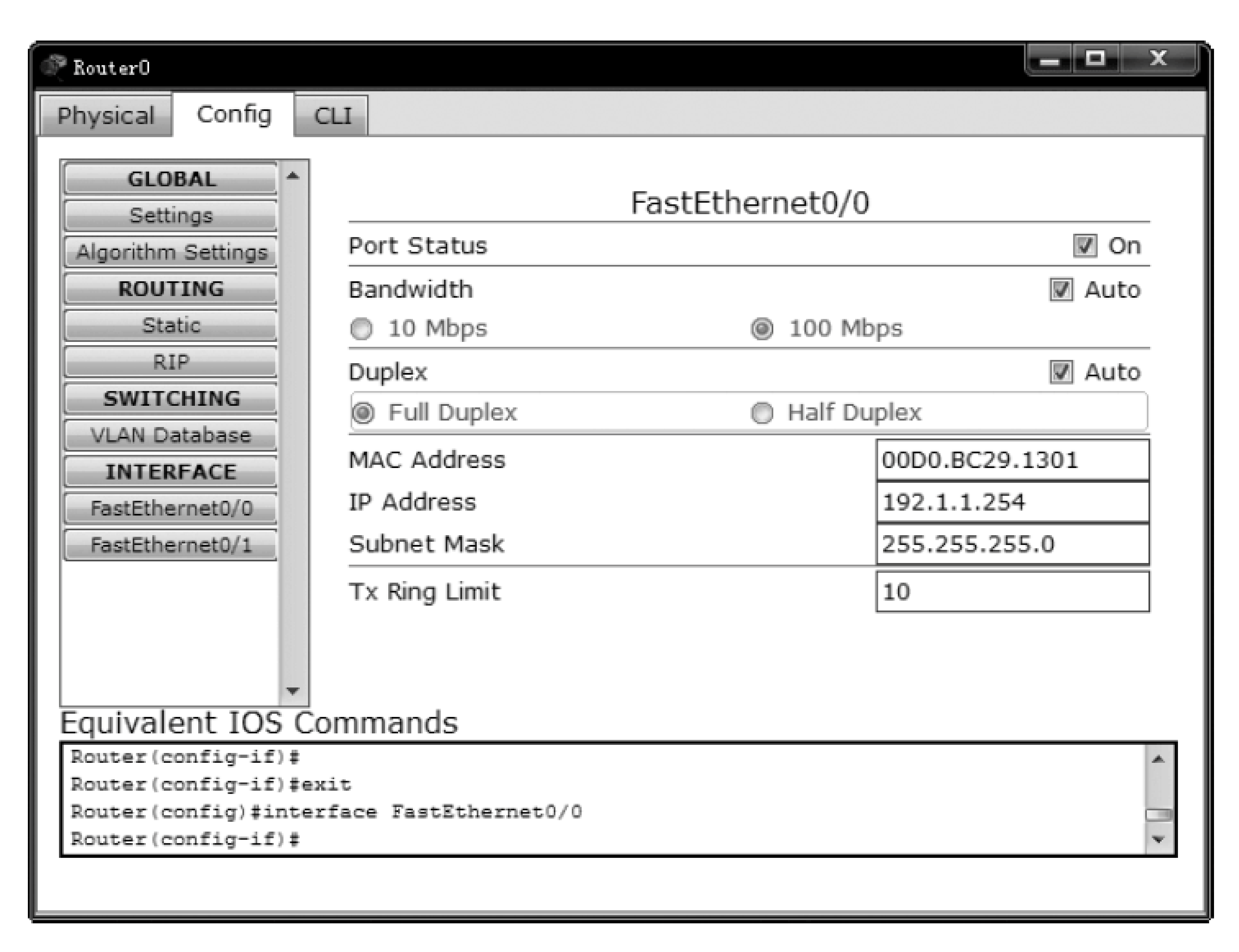


图 1.10　路由器接口配置界面

（3）完成路由器接口配置后，通过下述操作查看路由器 Router0 的路由表。单击公共工具栏中的查看图标，出现放大镜形状光标，移动光标到路由器 Router0，单击 Router0，出现图 1.13 所示的路由器控制信息表列表，单击 Routing Table（路由表），出现图 1.9 所示的 Router0 路由表。单击公共工具栏中的退出图标退出查看过程。

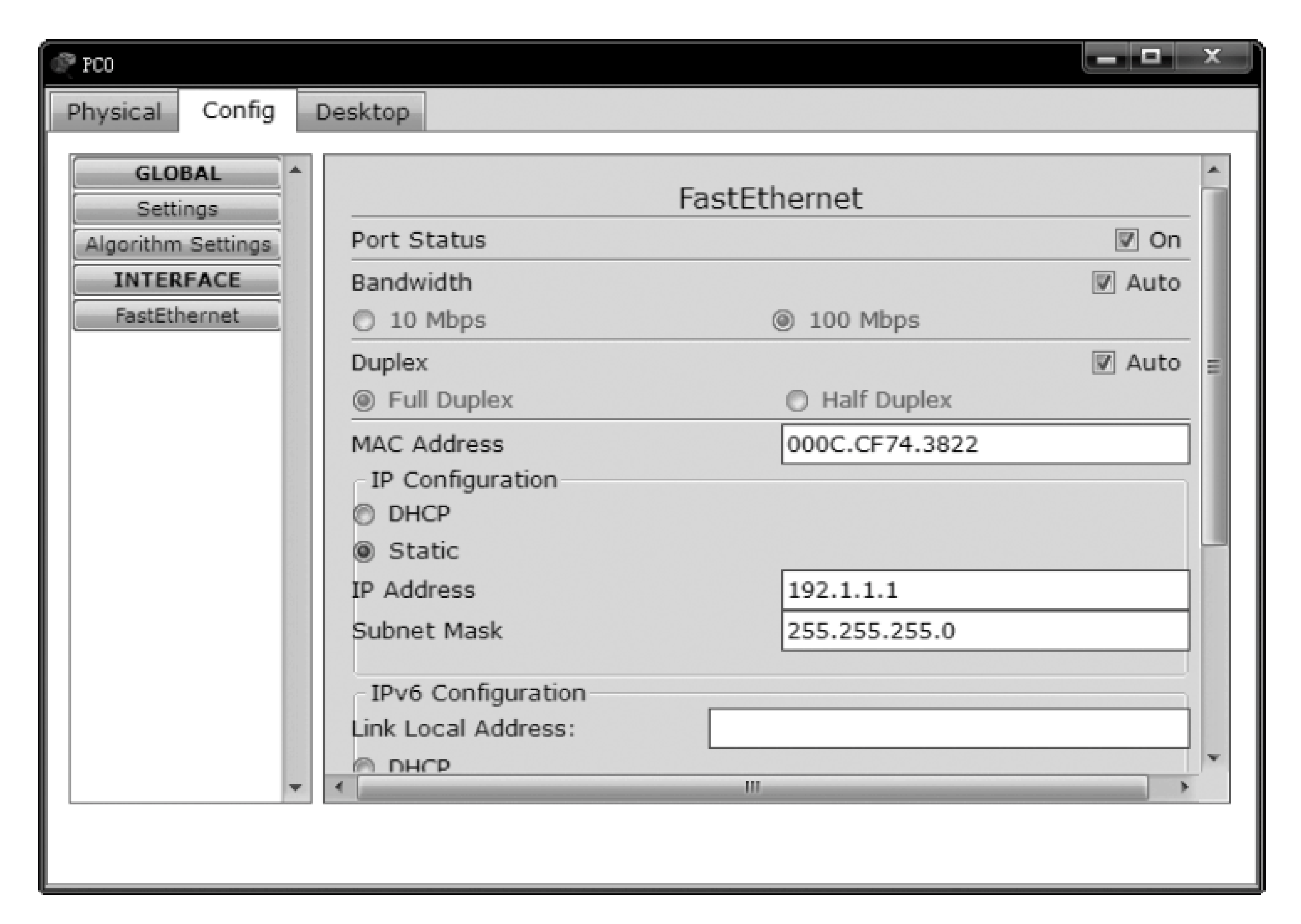


图 1.11　PC0 以太网接口 IP 地址和子网掩码配置界面

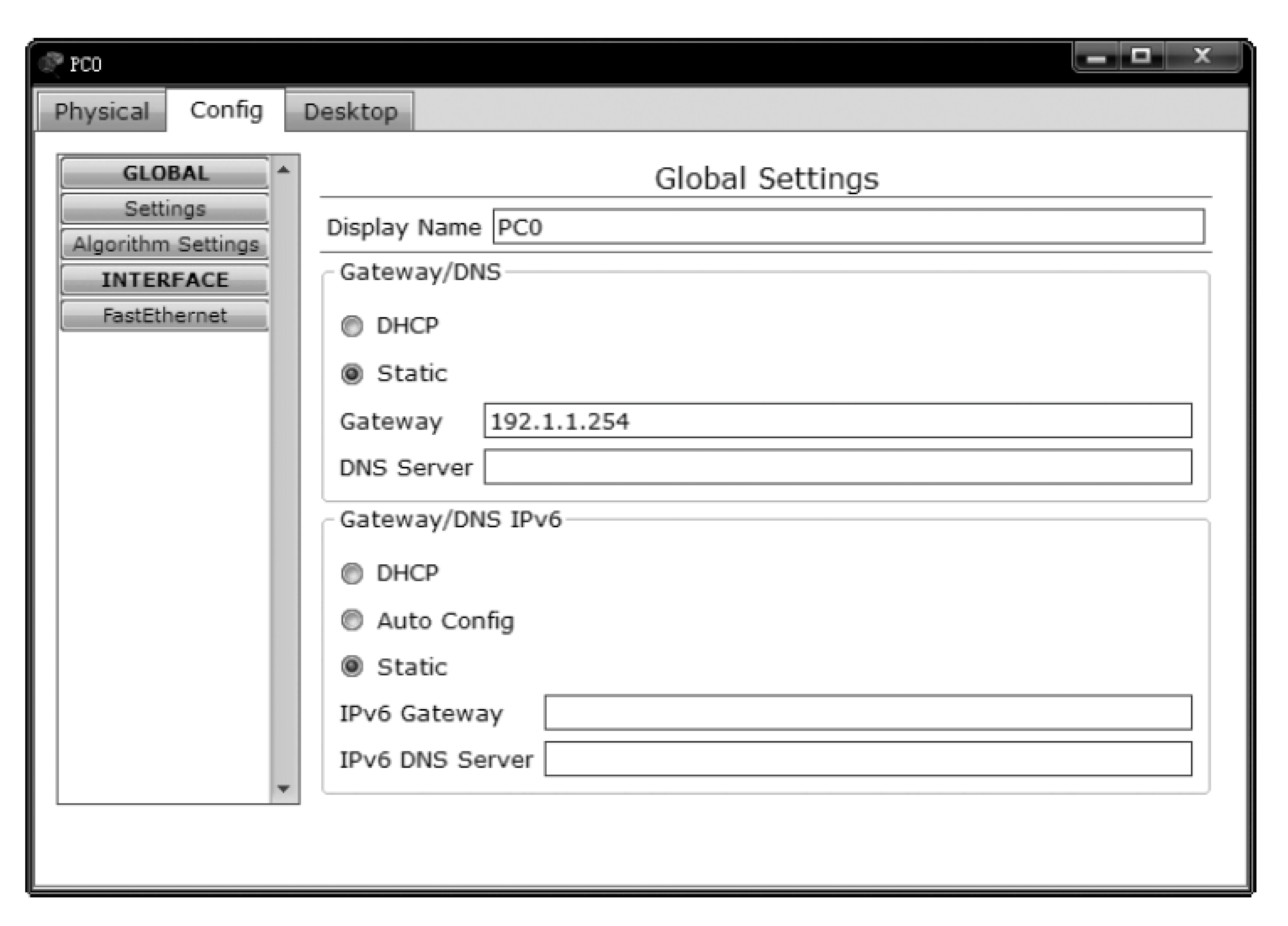


图 1.12　PC0 默认网关地址配置界面

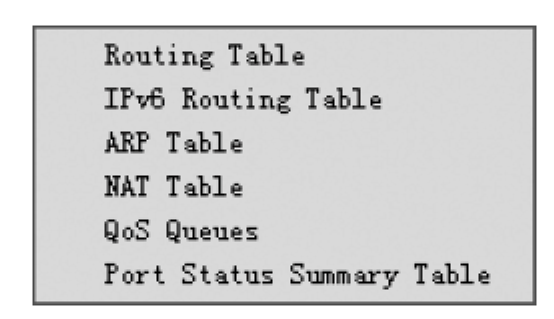


图 1.13　路由器控制信息表列表

（4）通过 Ping 操作验证 PC0、PC1 和 Server0 之间的连通性。

(5) 在 Router0 和 Switch1 之间插入集线器，用集线器互连 Router0、Switch1 和 hack 终端，如图 1.14 所示。进入模拟操作模式，单击公共工具栏中的复杂报文图标，在逻辑工作区出现信封形状光标，移动光标到 Server0，单击 Server0，出现图 1.15 所示的创建 PDU 界面，创建一个 Server0 至 PC0 IP 分组，启动 IP 分组 Server0 至 PC0 传输过程，发现 hack 终端能够嗅探到 Server0 传输给 PC0 的 IP 分组，如图 1.16 所示。其实，hack 终端能够嗅探到所有 PC0、PC1 与 Server0 之间传输的 IP 分组。

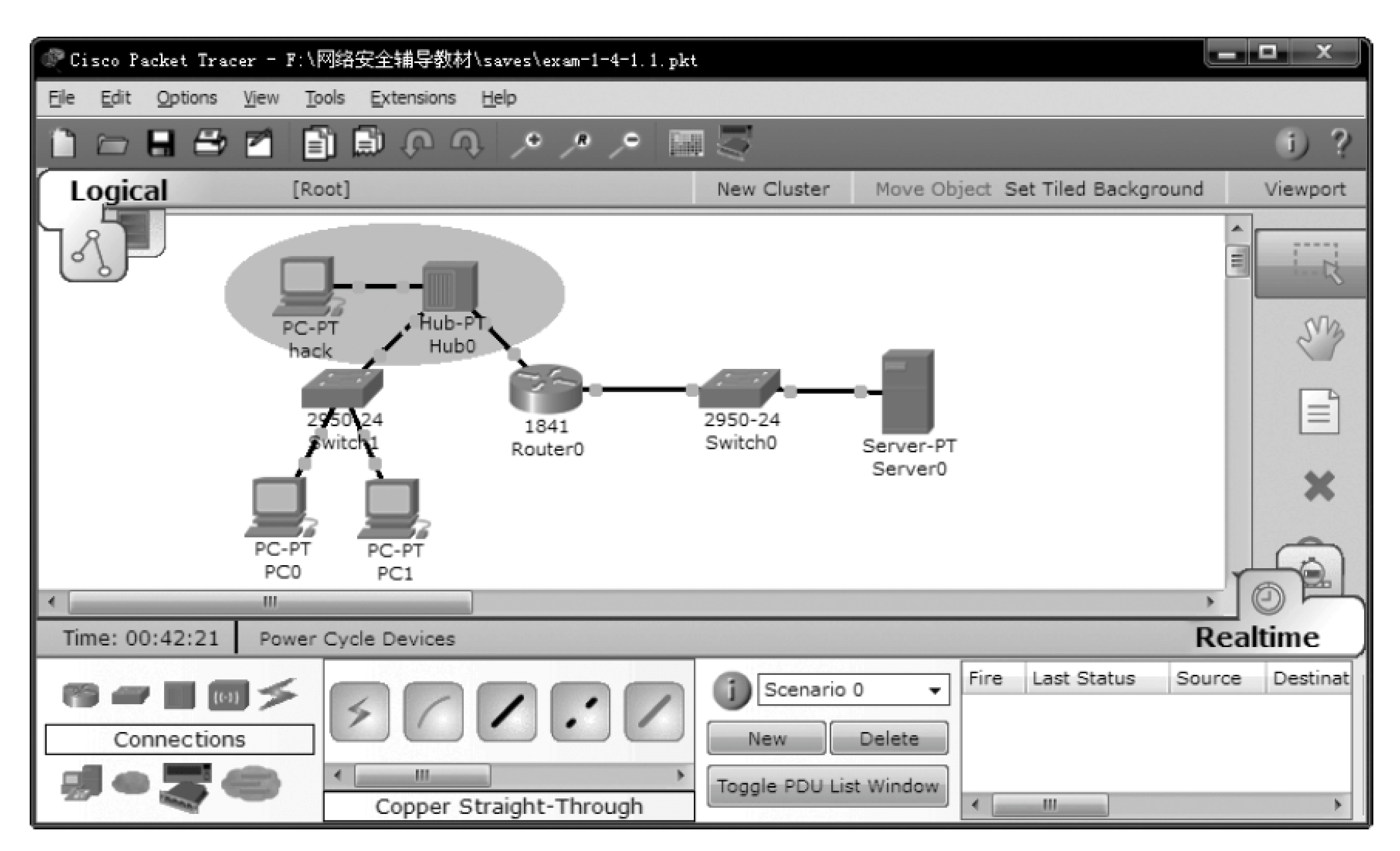


图 1.14　黑客信息嗅探攻击原理

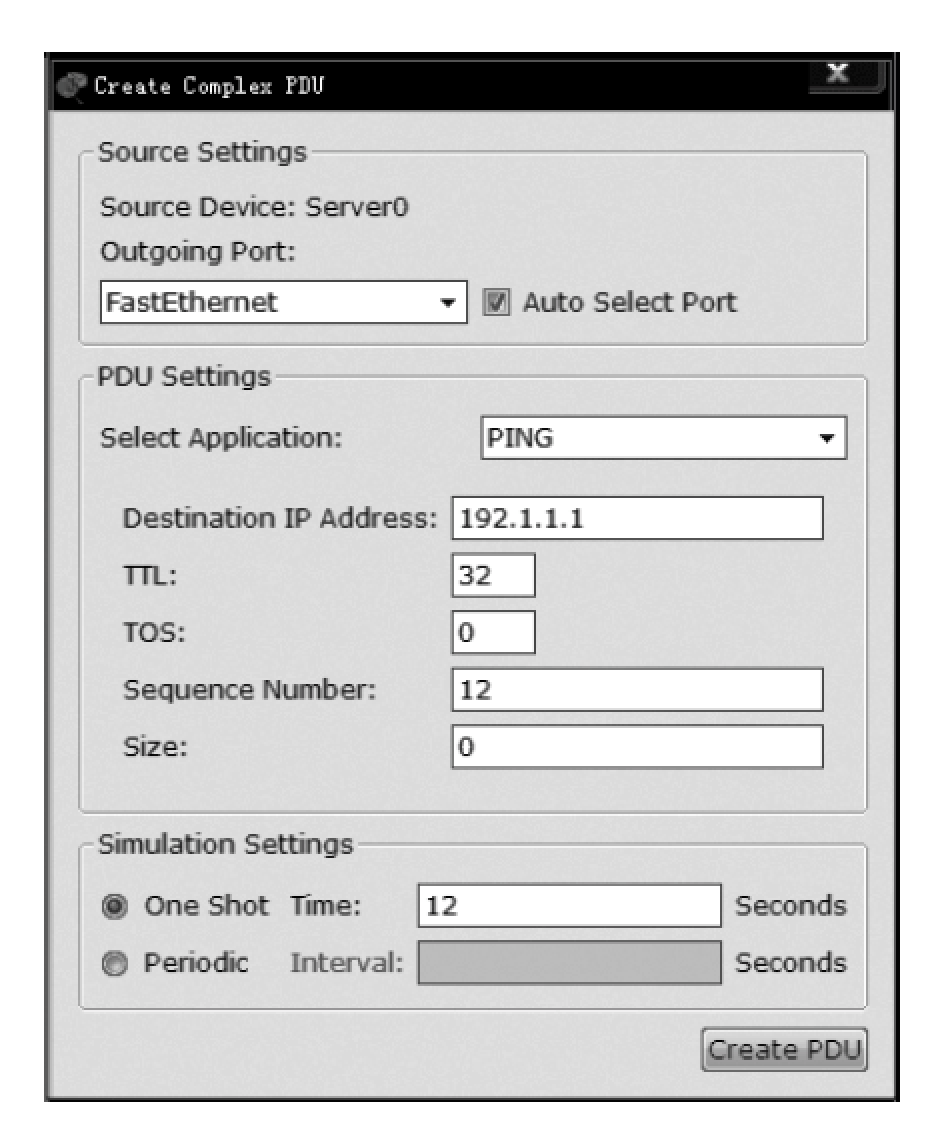


图 1.15　Server0 至 PC0 ICMP 消息

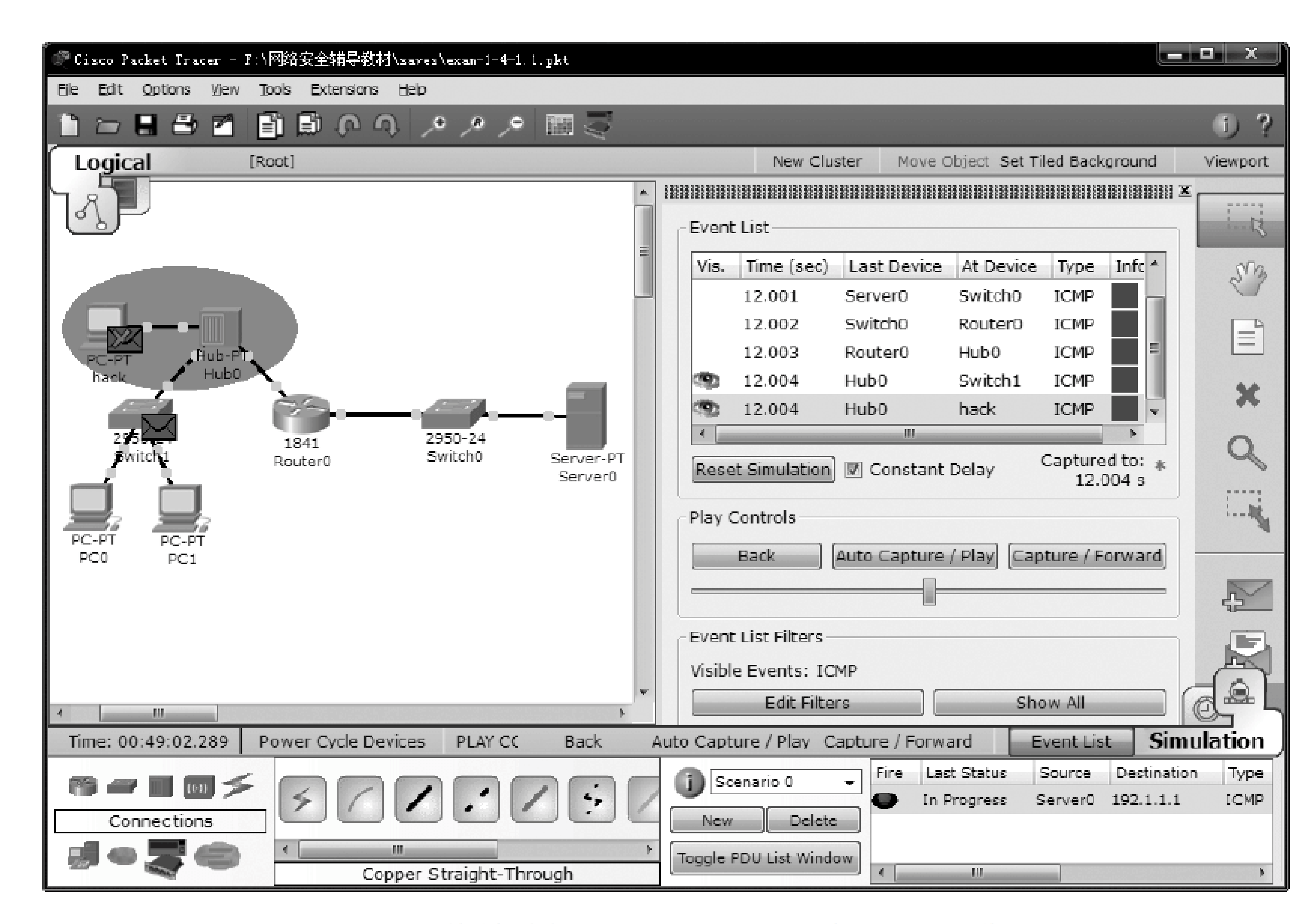


图 1.16 hack 终端嗅探 Server0 至 PC0 或 PC1 IP 分组过程

4. 路由器命令行配置过程

```
Router>enable                             (从用户模式命令提示符进入特权模式命令提示符)
Router#configure terminal                 (从特权模式命令提示符进入全局配置模式命令提示符)
Router(config)#interface FastEthernet0/0
                                          (进入接口配置模式,配置接口 FastEthernet0/0)
Router(config-if)#no shutdown             (开启接口 FastEthernet0/0)
Router(config-if)#ip address 192.1.1.254 255.255.255.0
                                          (配置接口 IP 地址和子网掩码)
Router(config-if)#exit                    (退出接口配置模式,返回到全局配置模式)
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
```

1.4.2 信息截获攻击实验

1. 实验内容

(1) 完成互连网络设计。

(2) 验证 IP 分组端到端传输机制。

(3) 验证交换机转发表(MAC Table)建立过程。

(4) 验证交换机转发 MAC 帧过程。

(5) 验证通过修改 MAC 地址截获 MAC 帧的机制。

2. 网络结构

网络结构如图 1.17 所示。如果黑客获知了某个终端的 MAC 地址,如终端 A 的

MAC 地址 MAC A，通过将自己网卡的 MAC 地址设置成 MAC A 来截获其他终端或路由器发送给终端 A 的 MAC 帧。信息截获攻击机制如下：如果黑客终端经常向交换机发送以 MAC A 为源 MAC 地址的 MAC 帧，交换机转发表中建立表明 MAC A 和连接黑客终端的端口之间绑定关系的转发项<MAC A，3>，3 是交换机连接黑客终端的端口的端口号。如果其他终端或路由器向终端 A 发送 MAC 帧，该 MAC 帧以 MAC A 为目的 MAC 地址，交换机将这样的 MAC 帧通过与 MAC A 绑定的端口转发出去，该 MAC 帧到达黑客终端，而不是终端 A。

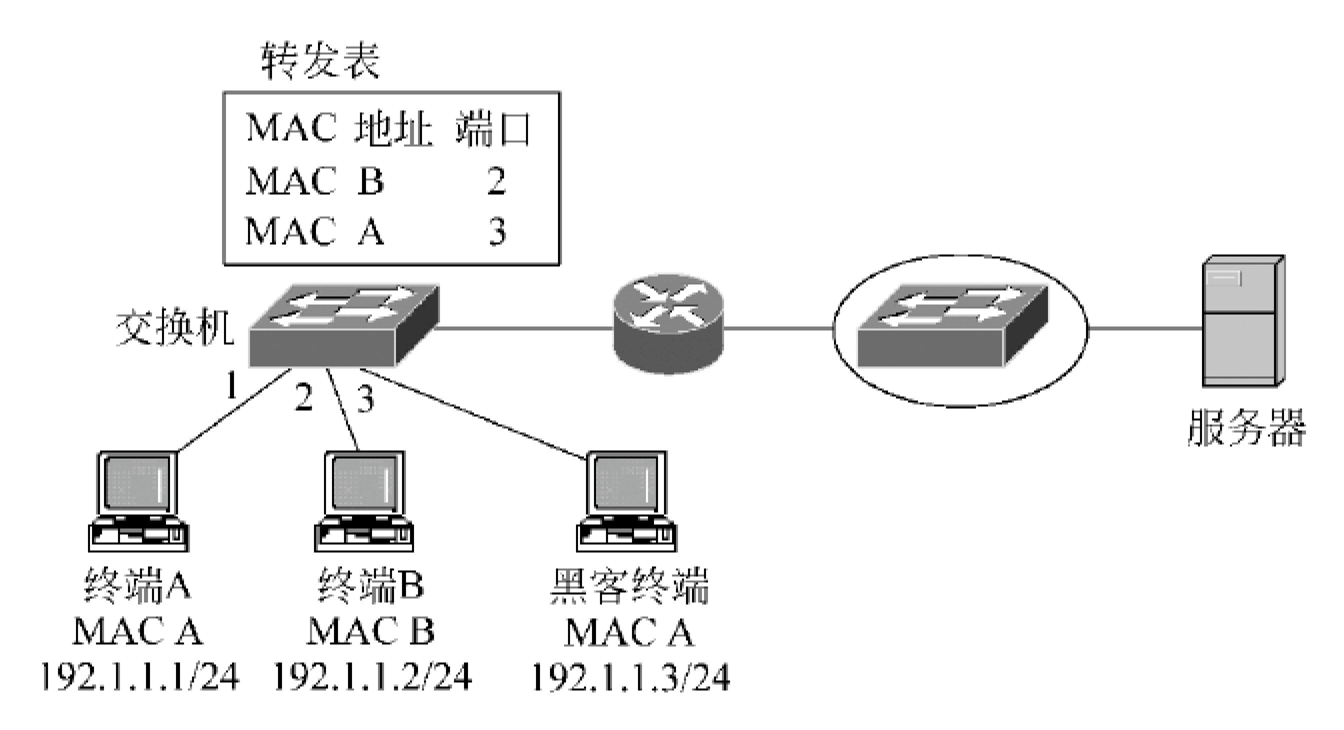


图 1.17　网络结构

3. 实验步骤

（1）启动 Packet Tracer，按照图 1.17 所示网络结构在逻辑工作区放置和连接设备，放置和连接设备后的逻辑工作区界面如图 1.18 所示。为路由器接口配置 IP 地址和子网掩码，同时为终端和服务器配置相应的 IP 地址、子网掩码和默认网关地址。

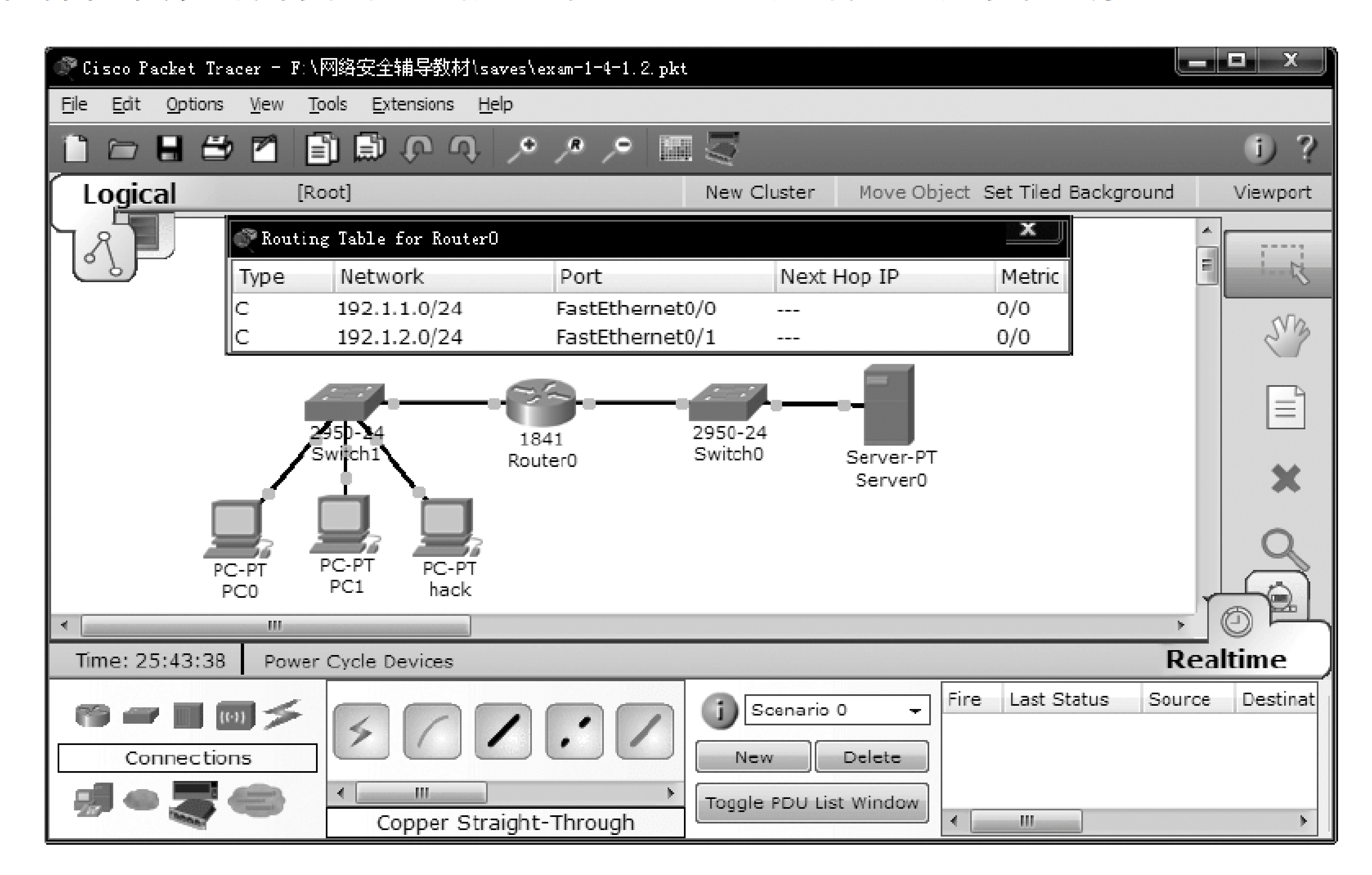


图 1.18　放置和连接设备后的逻辑工作区界面及路由表

（2）通过 Ping 操作，验证 PC0、PC1 和服务器之间的连通性。PC0 以太网接口的 MAC 地址为 000C.CF74.3822，如图 1.19 所示。完成 PC0、PC1 和服务器之间的 IP 分

组传输后，交换机 Switch1 的转发表如图 1.20 所示。MAC 地址 000C.CF74.3822 和端口 1 绑定在一起，端口 1 是交换机 Switch1 连接 PC0 的端口。

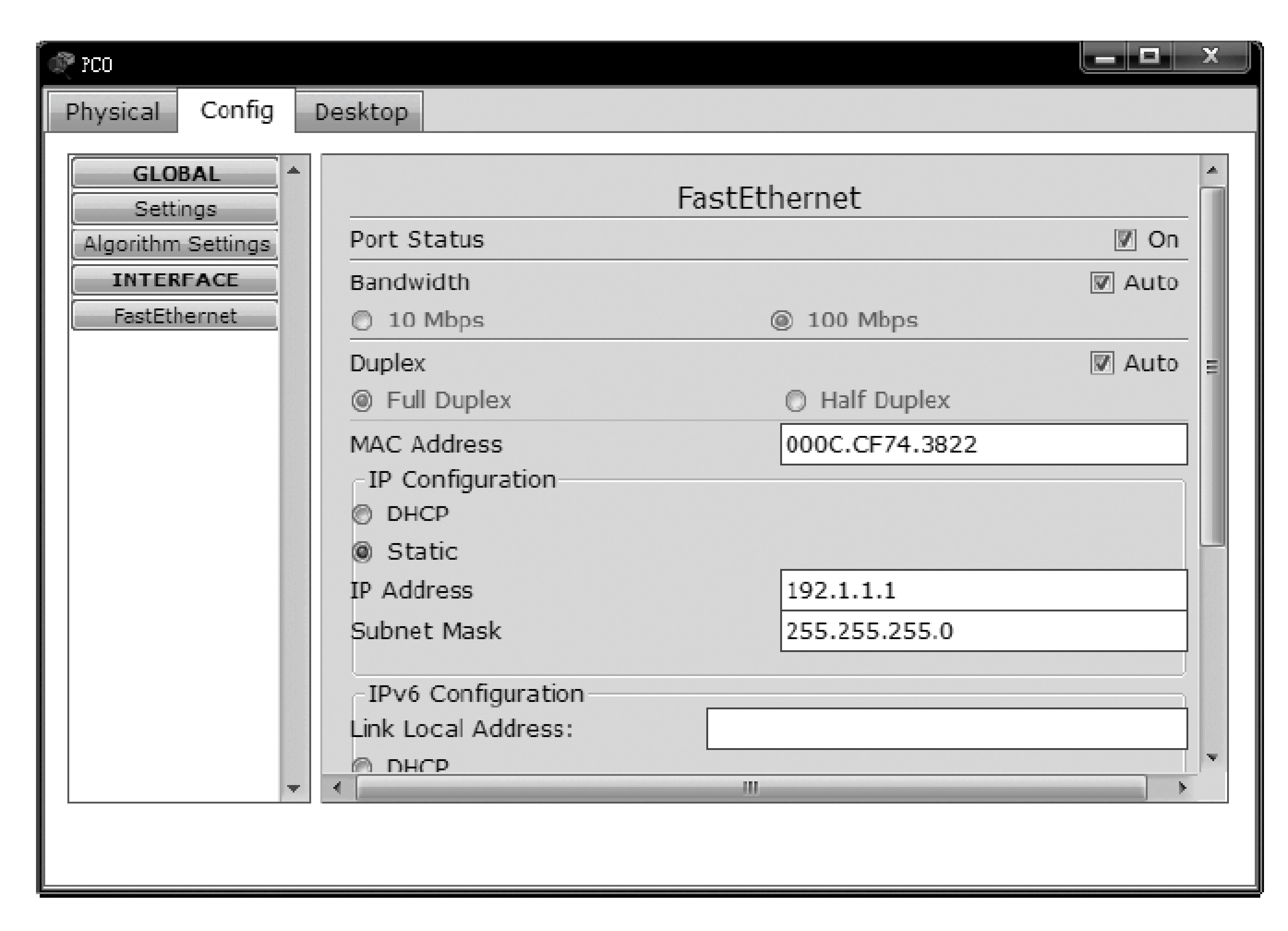
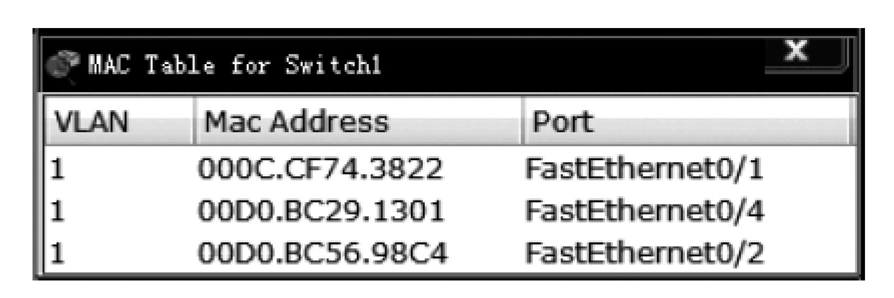


图 1.19 PC0 的 MAC 地址、IP 地址和子网掩码


MAC Table for Switch1

VLAN	Mac Address	Port
1	000C.CF74.3822	FastEthernet0/1
1	00D0.BC29.1301	FastEthernet0/4
1	00D0.BC56.98C4	FastEthernet0/2

图 1.20 正常的 Switch1 转发表

（3）假定黑客获知 PC0 的 MAC 地址，将 hack 终端的 MAC 地址修改为 PC0 的 MAC 地址 000C.CF74.3822，如图 1.21 所示。并发送以 MAC 地址 000C.CF74.3822 为

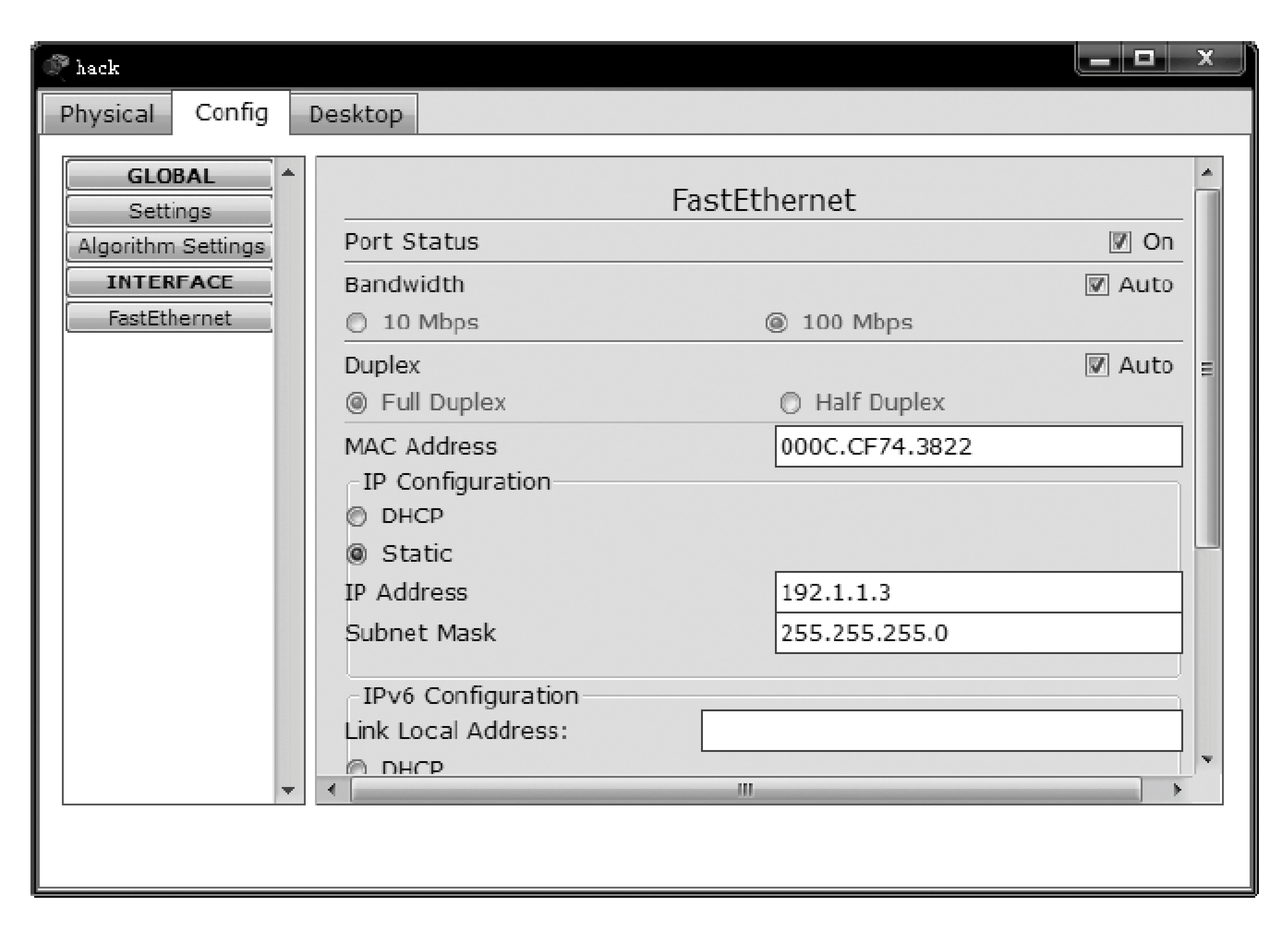


图 1.21 将 hack 终端的 MAC 地址设置为 PC0 的 MAC 地址

源地址的 MAC 帧,交换机 Switch1 转发表发生图 1.22 所示的转换。MAC 地址 000C.CF74.3822 和端口 3 绑定在一起,端口 3 是 Switch1 连接 hack 终端的端口。

MAC Table for Switch1

VLAN	Mac Address	Port
1	000C.CF74.3822	FastEthernet0/3
1	00D0.BC29.1301	FastEthernet0/4
1	00D0.BC56.98C4	FastEthernet0/2

图 1.22 错误的 Switch1 转发表

(4) 如果在 Server0 创建一个以 PC0 的 IP 地址 192.1.1.1 为目的地址的 IP 分组,该 IP 分组在 Router0 至 PC0 的传输过程中被封装为以 PC0 的 MAC 地址 000C.CF74.3822 为目的地址的 MAC 帧,如图 1.23 所示。但该 MAC 帧经过交换机 Switch1 转发后,不是经过端口 1 到达 PC0,而是经过端口 3 到达 hack 终端,如图 1.24 所示。只要 hack 终端经常发送以 MAC 地址 000C.CF74.3822 为源地址的 MAC 帧,交换机 Switch1 的转发表中与 MAC 地址 000C.CF74.3822 绑定的端口一直是交换机连接 hack 终端的端口,而不是连接 PC0 的端口。

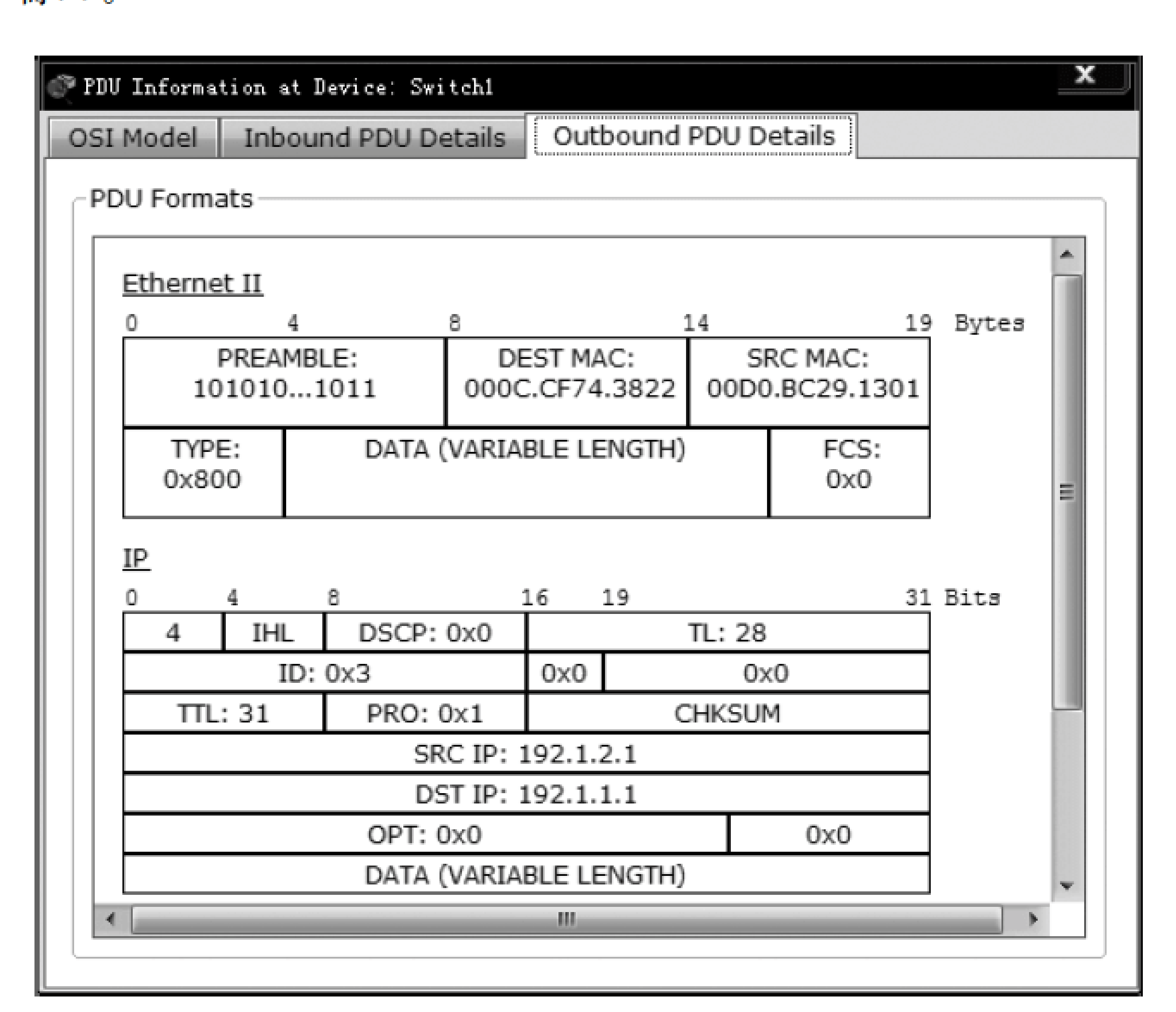


图 1.23 Server0→PC0 IP 分组 Router0 至 PC0 段的 MAC 帧格式

1.4.3 拒绝服务攻击实验

1. 实验内容

(1) 验证源 IP 地址欺骗攻击机制。

(2) 验证定向广播传输过程。

(3) 验证拒绝服务攻击过程。

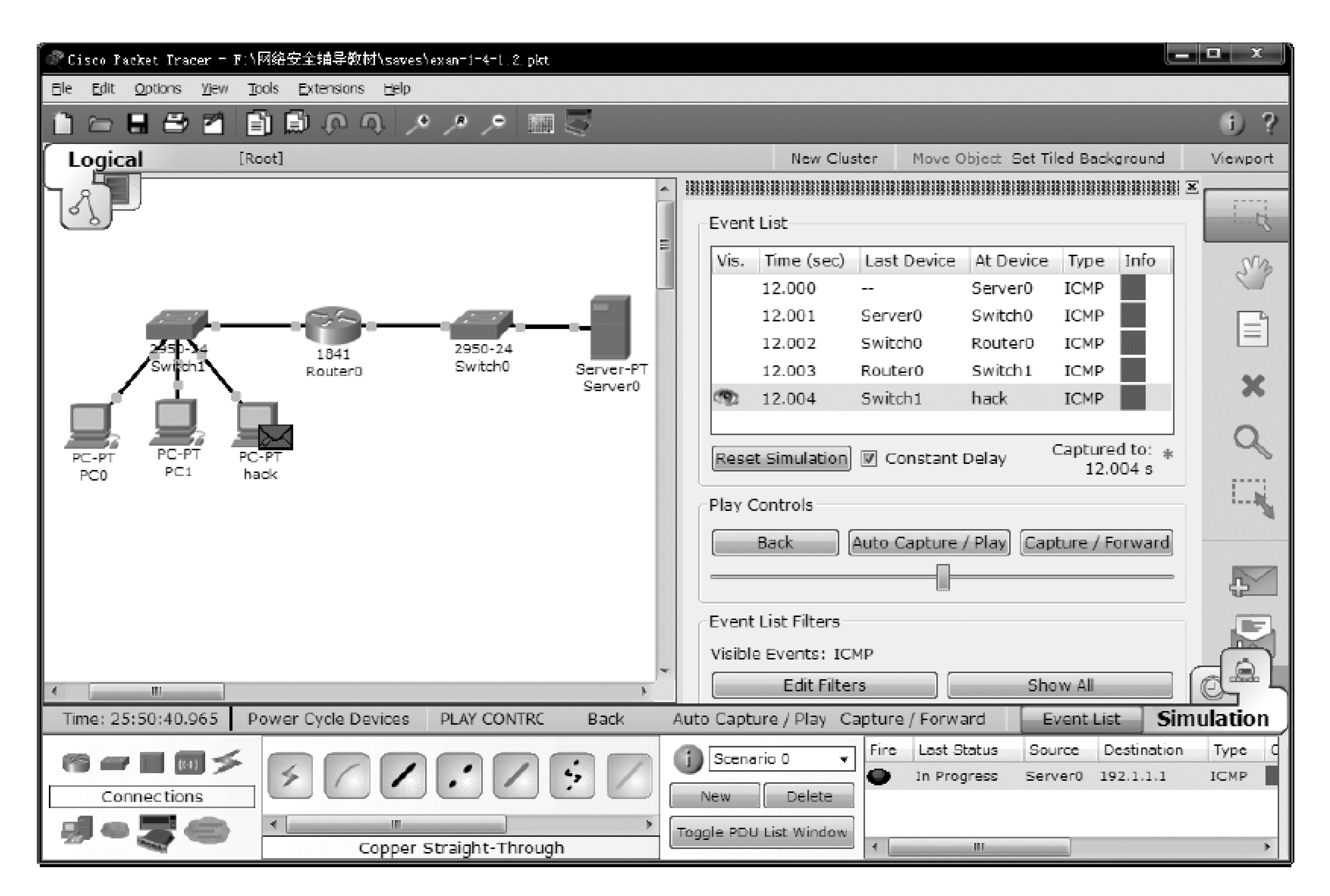


图 1.24　Server0 至 PC0 IP 分组被传输到 hack 终端

2. 网络结构

网络结构如图 1.25 所示。黑客终端创建并发送一个以 192.1.2.1 为源 IP 地址、以 192.1.1.255 为目的 IP 地址的 ICMP ECHO 请求报文，由于封装该 ICMP ECHO 请求报文的 IP 分组的目的地址是定向广播地址，因此被连接在网络 192.1.1.0/24 中的所有终端接收，所有接收该 ICMP ECHO 请求报文的终端向 IP 地址为 192.1.2.1 的服务器发送 ICMP ECHO 响应报文，大量 ICMP ECHO 响应报文到达服务器，消耗掉服务器连接网络的链路的带宽和服务器的处理能力，导致服务器无法正常提供服务。

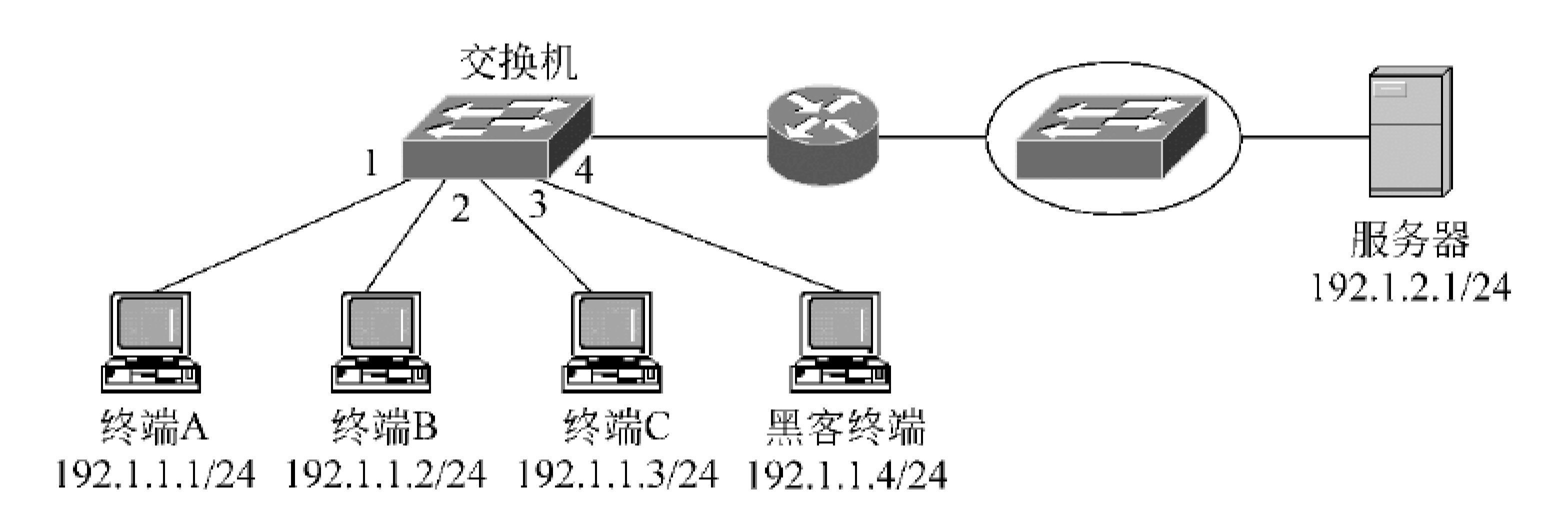


图 1.25　实施拒绝服务攻击网络结构

3. 实验步骤

（1）启动 Packet Tracer，按照图 1.25 所示网络结构在逻辑工作区放置和连接网络设备，放置和连接网络设备后的逻辑工作区界面如图 1.26 所示。

（2）按照图 1.25 所示网络配置信息为路由器接口配置 IP 地址和子网掩码，为终端和服务器配置 IP 地址、子网掩码和相应的默认网关地址。

（3）进入模拟操作模式，hack 终端创建一个图 1.27 所示的以 192.1.2.1 为源 IP 地址、192.1.1.255 为目的 IP 地址的 ICMP ECHO 请求报文，该 ICMP ECHO 请求报文到

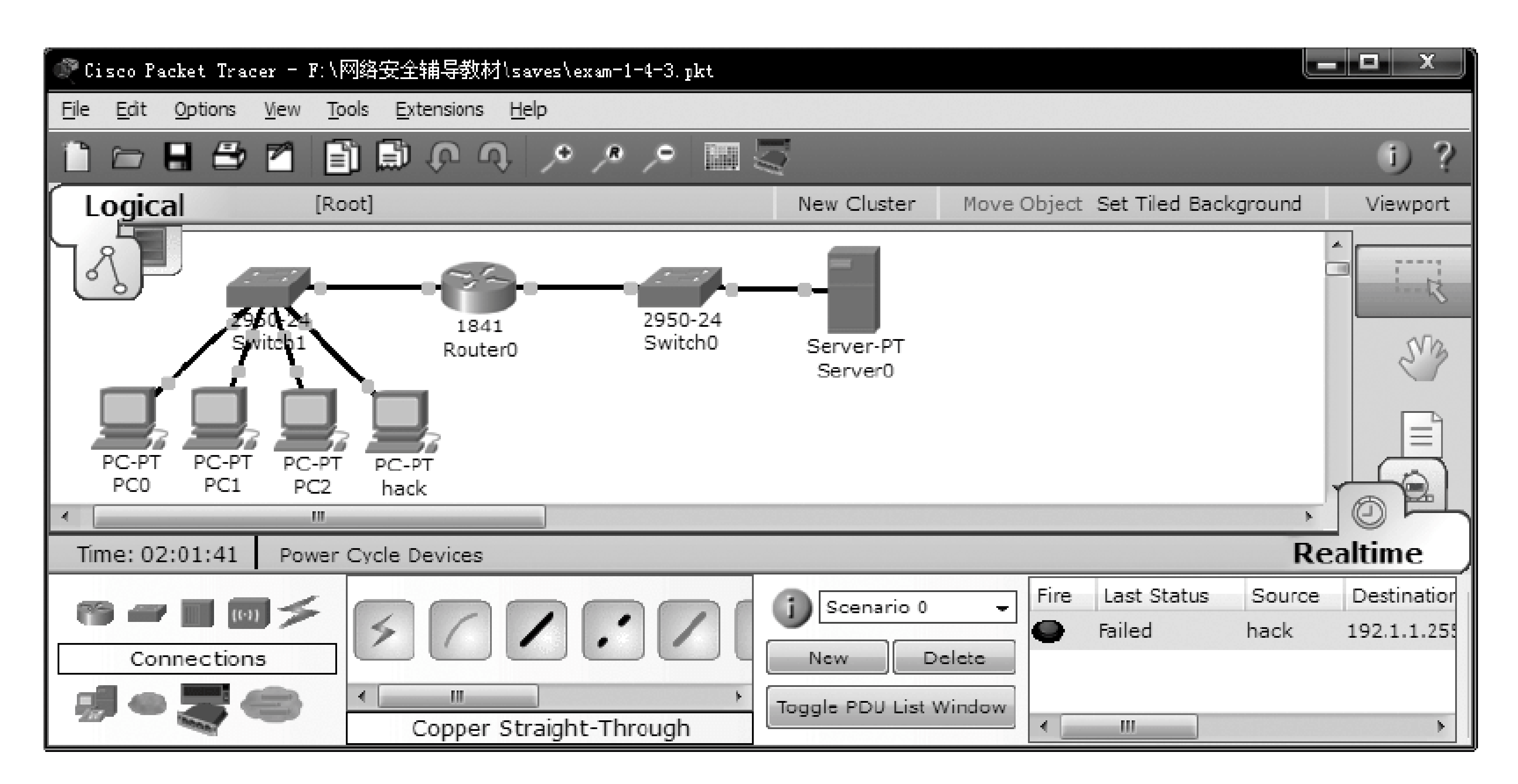


图 1.26　放置和连接设备后的逻辑工作区界面

达网络 192.1.1.0/24 中的所有终端，如图 1.28 所示。

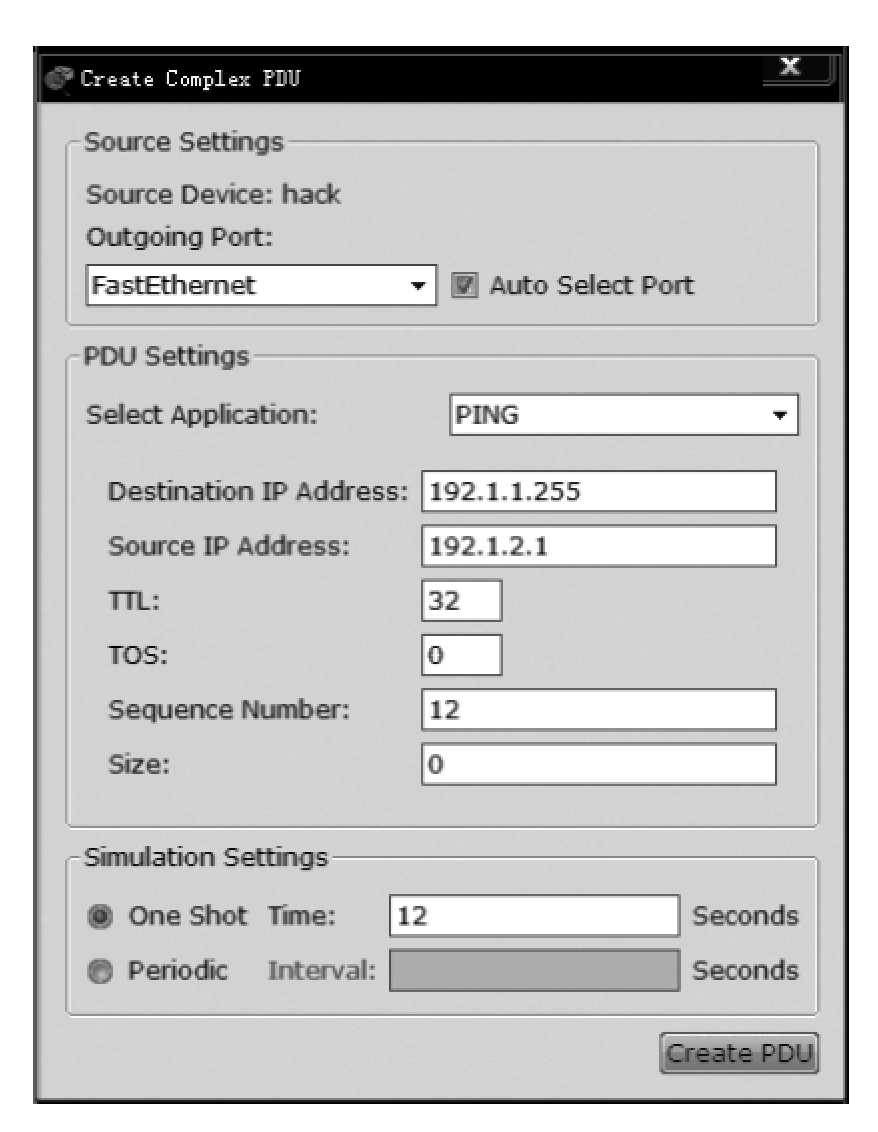


图 1.27　hack 终端创建的 ICMP ECHO 请求报文

（4）所有接收该 ICMP ECHO 请求报文的终端向 IP 地址为 192.1.2.1 的服务器发送 ICMP ECHO 响应报文，如图 1.29 所示。

1.4.4　路由项欺骗攻击实验

1．实验内容

（1）验证路由项欺骗攻击过程。

（2）配置路由器。

（3）验证路由表生成过程。

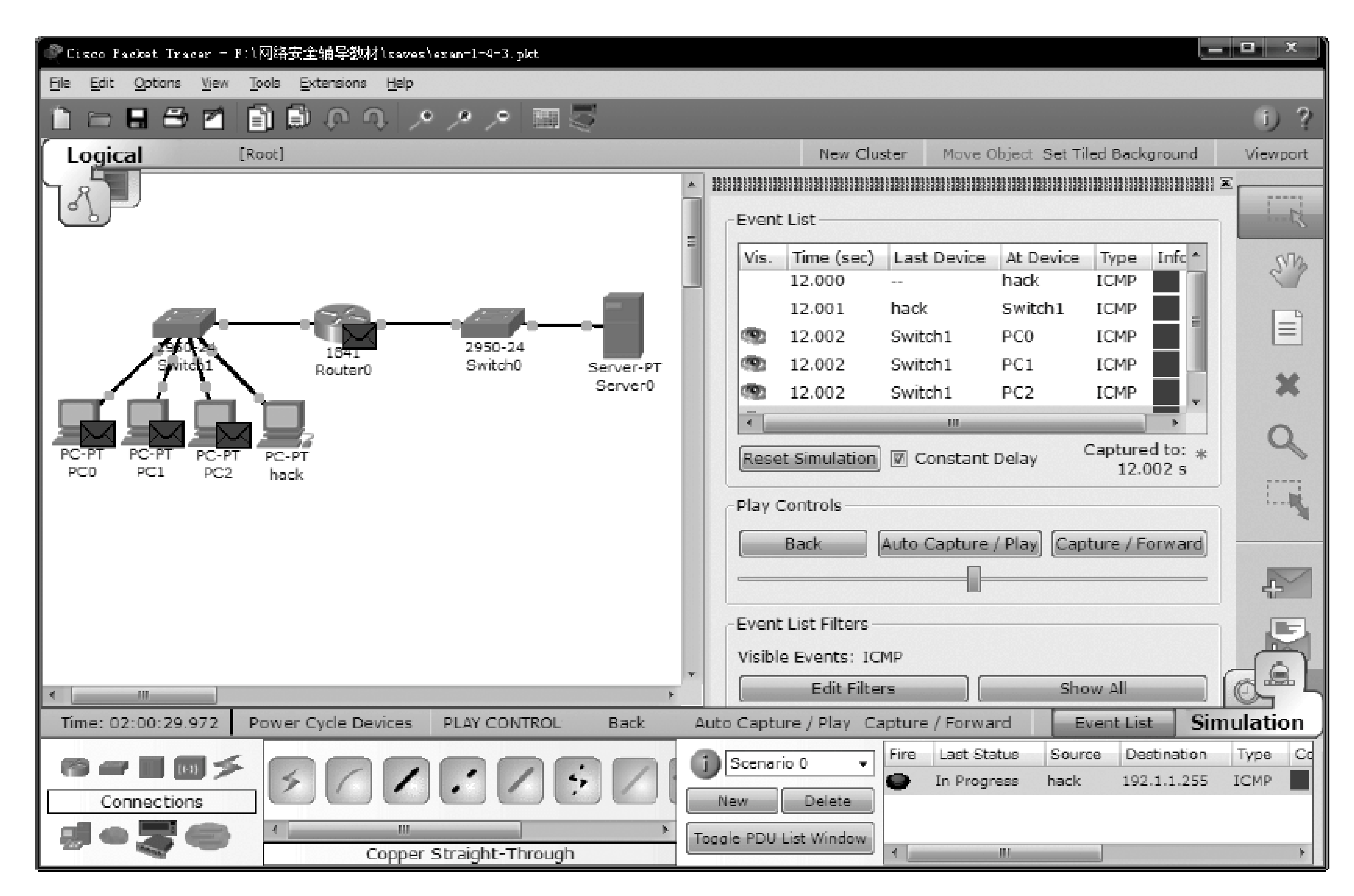


图 1.28 hack 终端发送的 ICMP ECHO 请求报文到达同一网络内的所有终端

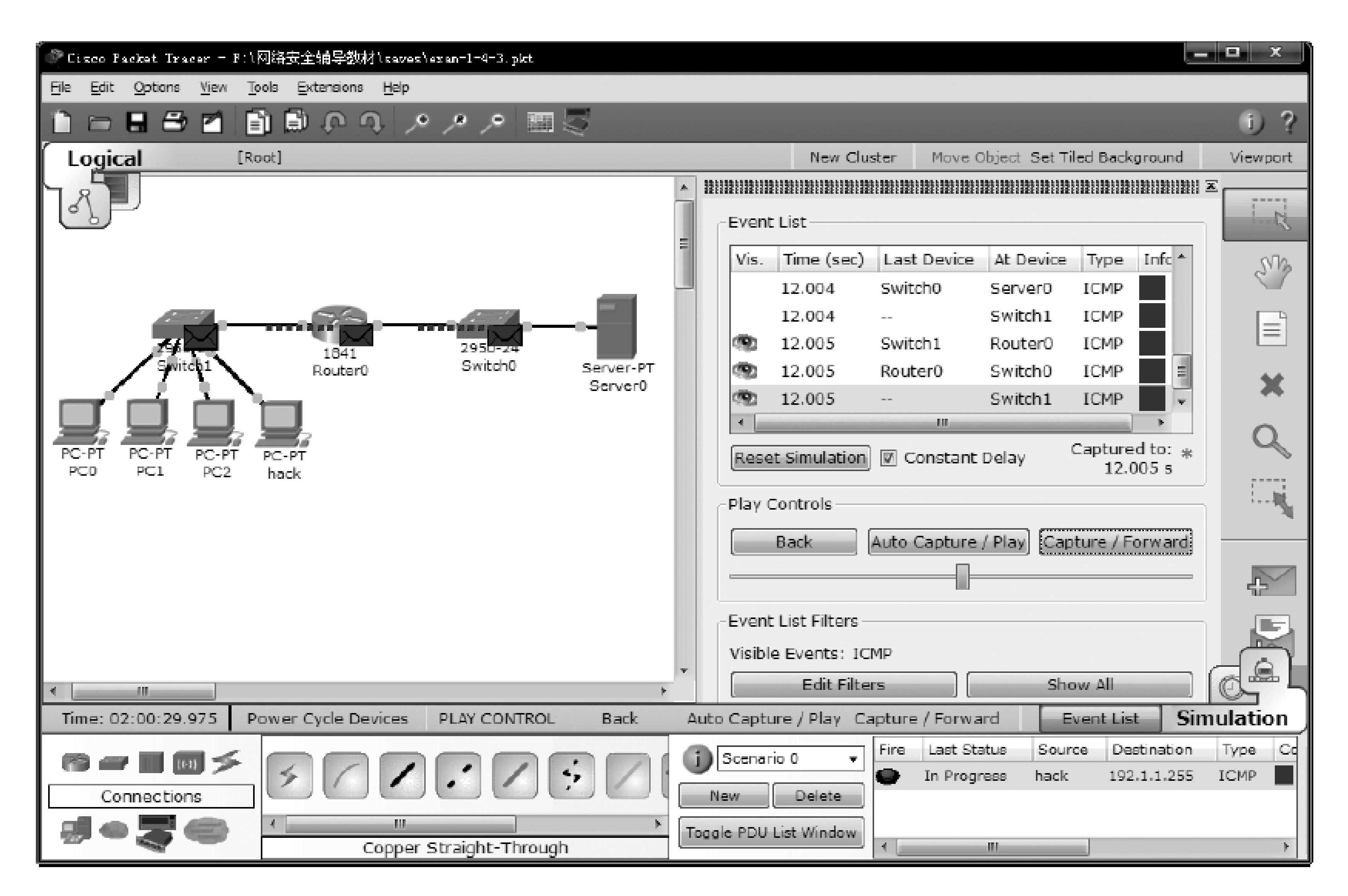


图 1.29 所有终端向 Server0 发送 ICMP ECHO 响应报文

2. 网络结构

针对图 1.30 所示的网络结构，路由器 R1 通过路由协议生成的正确路由表如图 1.30 中 R1 正确路由表所示。这种情况下，终端 A 发送给终端 B 的 IP 分组将沿着终端 A→路由器 R1→路由器 R2→路由器 R3→终端 B 的传输路径到达终端 B。如果某个入侵者想截获连接在网络 192.1.1.0/24 上的终端发送给连接在网络 192.1.4.0/24 上的终端的 IP 分组，通过接入网络 192.1.2.0/24 中的入侵路由器发送一个以入侵路由器 IP 地址 192.1.2.252 为源 IP 地址、组播地址 224.0.0.9 为目的 IP 地址的路由消息，该路由消息

伪造了一项入侵路由器直接和网络 192.1.4.0/24 连接的路由项(目的网络为 192.1.4.0/24,距离为 1),和入侵路由器连接在同一网络上的路由器 R1 和 R2 均接收到该路由消息。对于路由器 R1 而言,由于伪造路由项给出的到达网络 192.1.4.0/24 的距离最短,将通往网络 192.1.4.0/24 传输路径上的下一跳路由器改为入侵路由器,如图 1.30 中 R1 错误路由表所示,并导致路由器 R1 将所有连接在网络 192.1.1.0/24 上的终端发送给连接在网络 192.1.4.0/24 上的终端的 IP 分组错误地转发给入侵路由器。

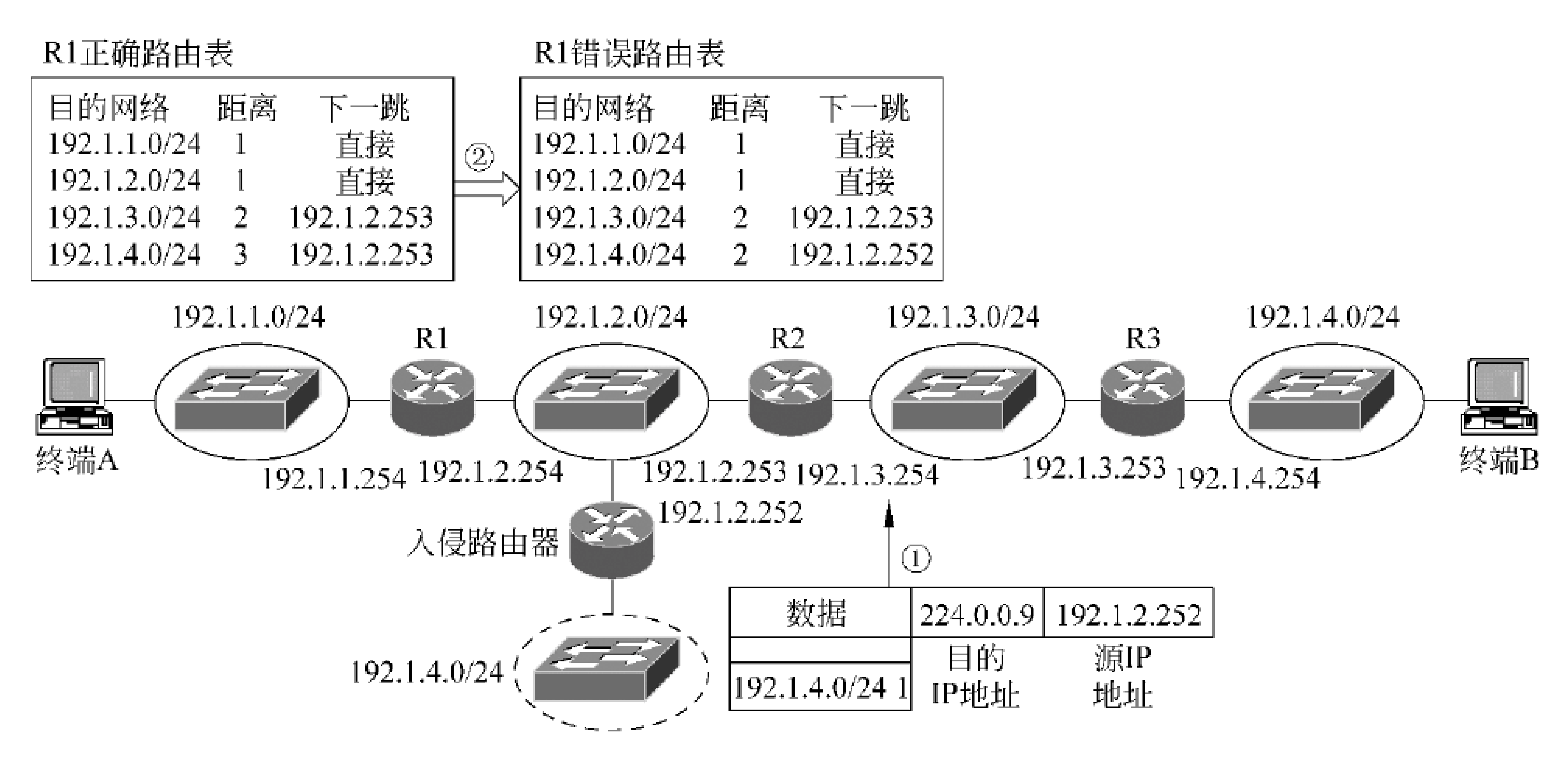


图 1.30　实施路由项欺骗攻击网络结构

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 1.30 所示的网络结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图 1.31 所示。

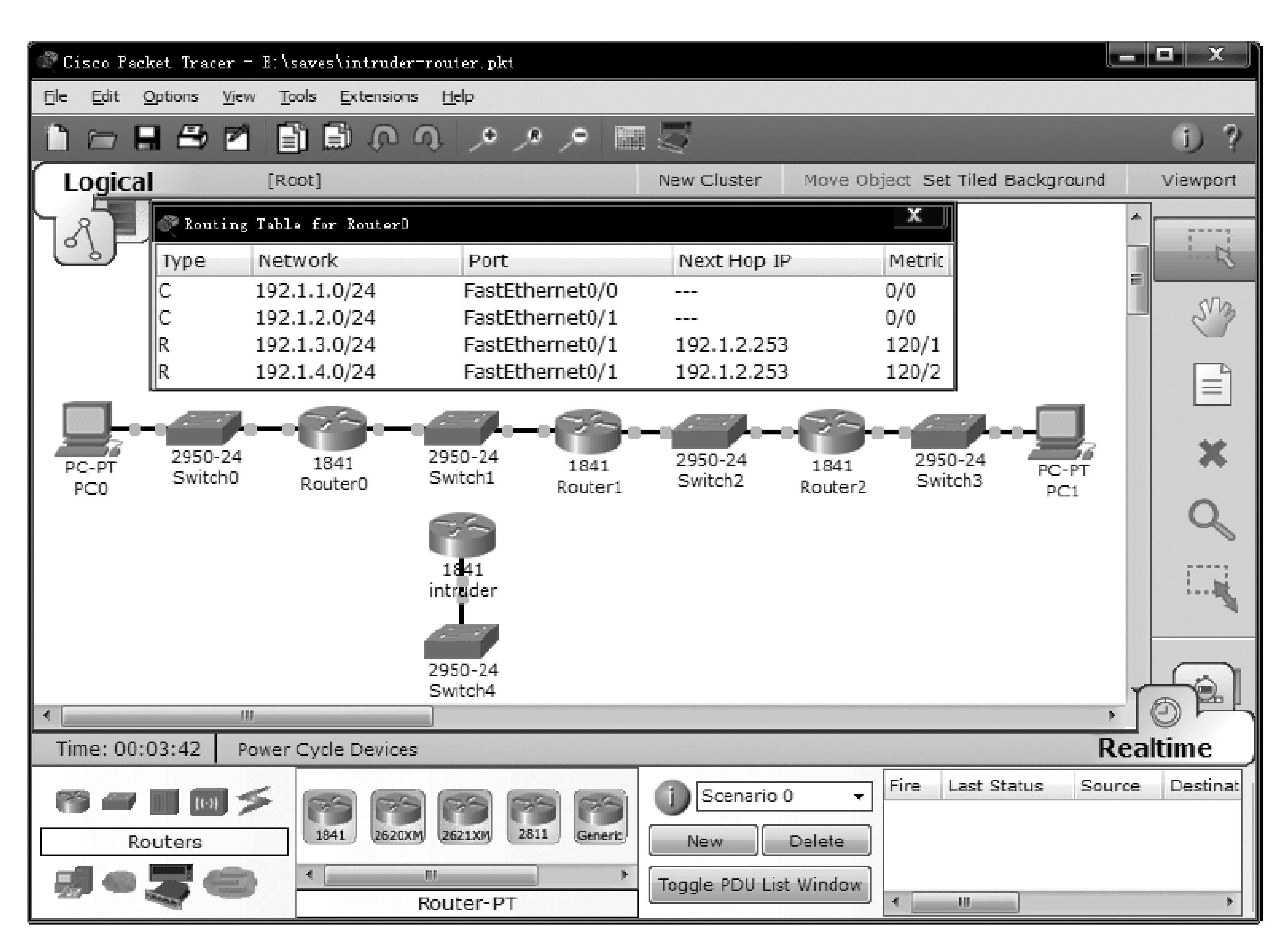


图 1.31　放置和连接设备后的逻辑工作区界面及 Router0 准确的路由表

(2) 完成路由器接口 IP 地址和子网掩码配置，同时启动 RIP，输入路由器直接相连的网络的网络地址。接下来检查路由器建立的路由表(图 1.31 给出路由器 Router0 建立的路由表，由于 Cisco 将直接相连的网络的距离设定为 0，图 1.31 中路由项的距离与图 1.30 中的距离差 1)。

(3) 将路由器 intruder 连接到网络 192.1.2.0/24，将连接网络 192.1.2.0/24 的接口的 IP 地址和子网掩码配置为 192.1.2.252/24。将另一个接口的 IP 地址和子网掩码配置为 192.1.4.254/24，表明该路由器直接和网络 192.1.4.0/24 相连。在路由器 intruder 启动 RIP，输入路由器 intruder 直接相连的网络的网络地址后，路由器 Router0 的路由表如图 1.32 所示，将通往网络 192.1.4.0/24 的传输路径的下一跳变为路由器 intruder。

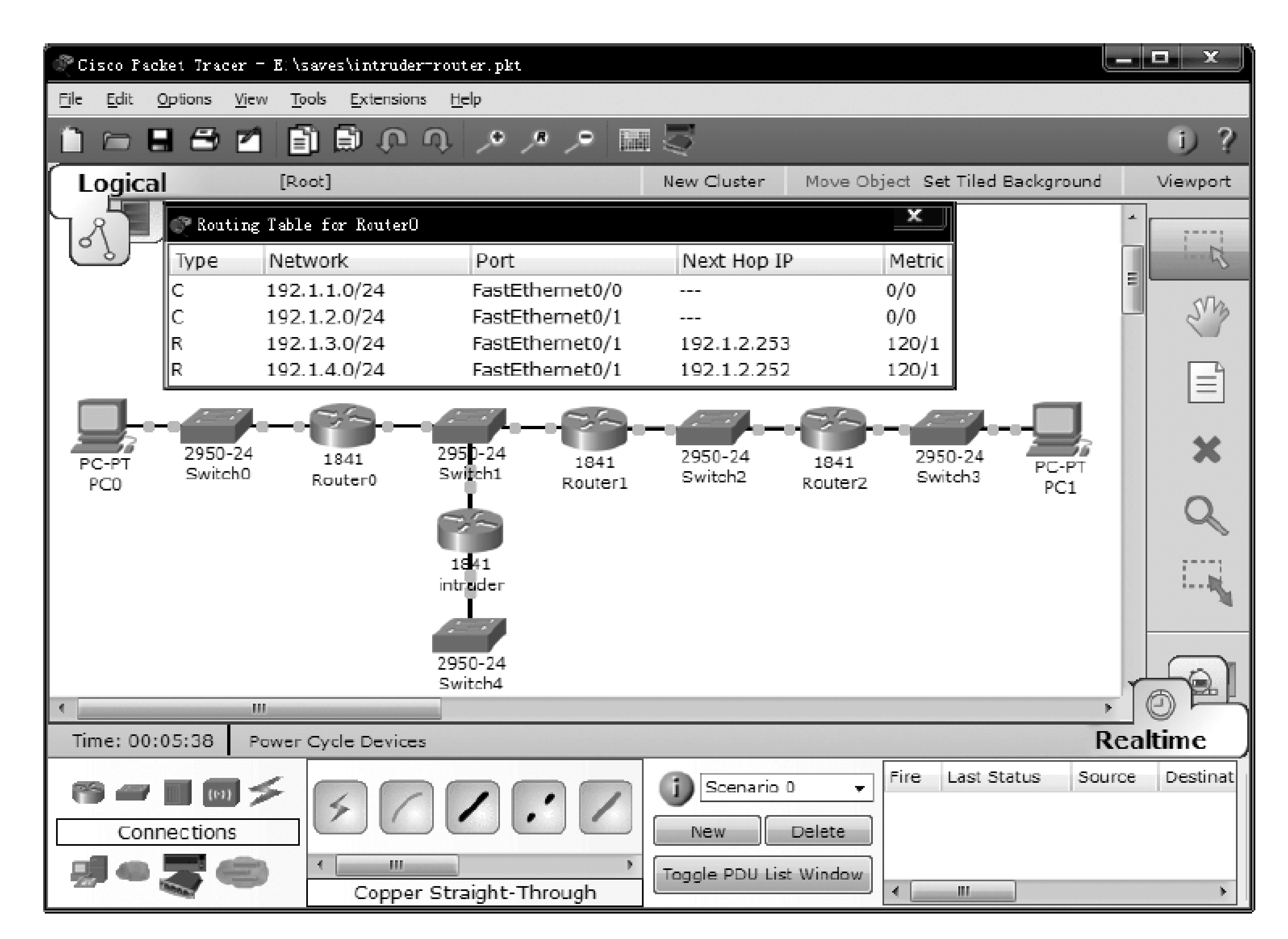


图 1.32 Router0 错误的路由表

(4) 进入模拟操作模式，在 PC0 创建并发送图 1.33 所示的以 PC0 的 IP 地址 192.1.1.1 为源地址、PC1 的 IP 地址 192.1.4.1 为目的地址的 ICMP ECHO 请求报文。结果发现路由器 Router0 将该 ICMP ECHO 请求报文转发给路由器 intruder，如图 1.34 所示。

Create Complex PDU
Source Settings
Source Device: PC0
Outgoing Port:
FastEthernet
Auto Select Port
PDU Settings
Select Application: PING
Destination IP Address: 192.1.4.1
Source IP Address: 192.1.1.1
TTL: 32
TOS: 0
Sequence Number: 12
Size: 0
Simulation Settings
One Shot Time: 12 Seconds
Periodic Interval: Seconds
Create PDU

图 1.33 PC0 至 PC1 的 IP 分组格式

4. 路由器命令行配置过程

(1) 路由器 Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.253 255.255.
```

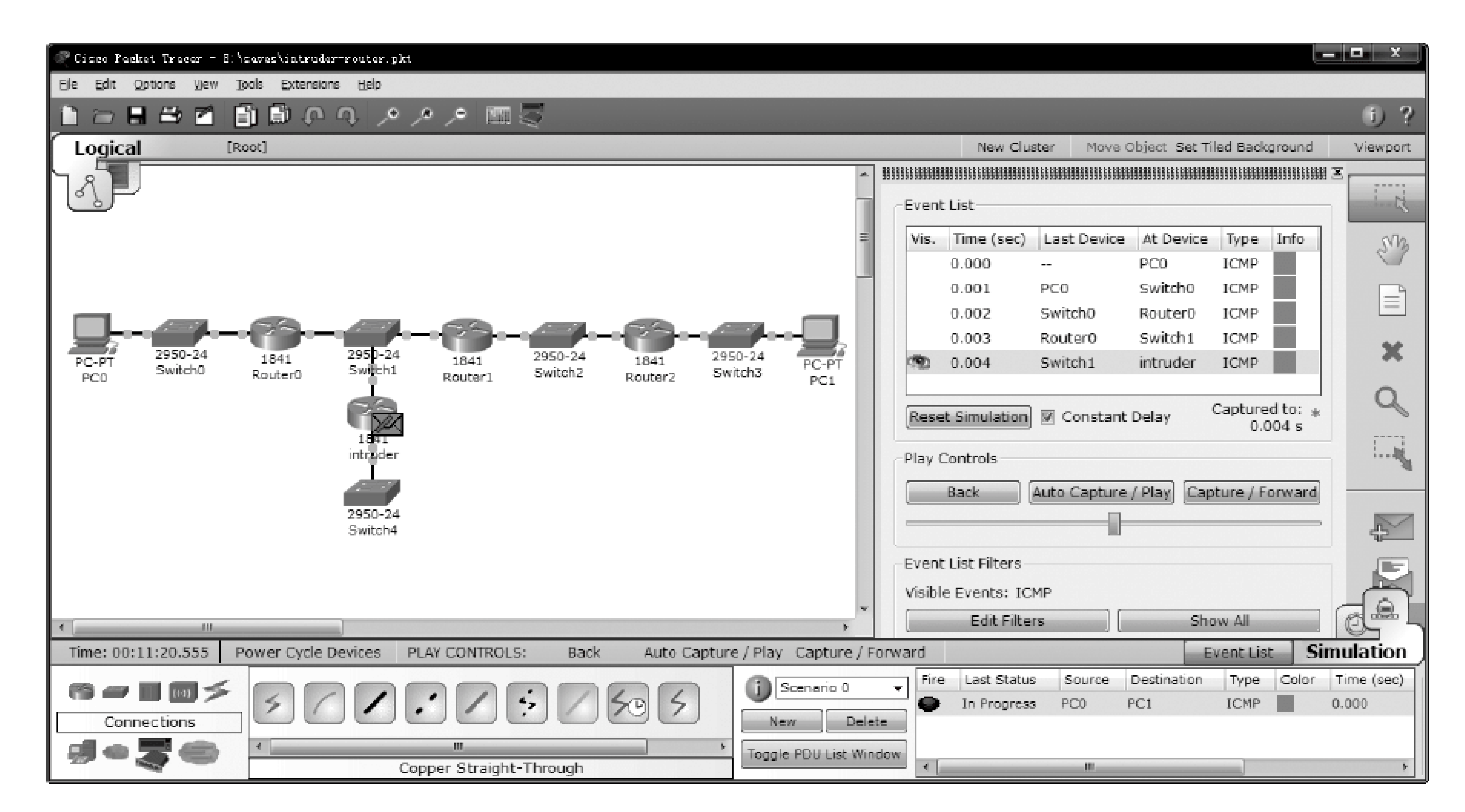


图 1.34　Router0 错误地将 PC0 至 PC1 的 IP 分组转发给 intruder

```
255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.3.0
Router(config-router)#network 192.1.4.0
Router(config-router)#exit
```

注意：路由器 Router0、Router1 的命令行配置过程与此相似，不再赘述。

(2) 路由器 intruder 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.252 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.4.0
                                  (路由器 intruder 一方面直接连接网络 192.1.2.0/24,
```

```
                                 另一方面伪造直接和网络 192.1.4.0/24 相连)
Router(config-router)#exit
```

1.4.5 DHCP 欺骗攻击实验

1. 实验内容

(1) 完成 DHCP 服务器配置过程。

(2) 验证 DHCP 自动配置网络信息机制。

(3) 验证 DHCP 欺骗攻击机制。

(4) 验证信息截获过程。

2. 网络结构

网络结构如图 1.35 所示。黑客伪造一个 DHCP 服务器,并将其接入以太网中,伪造的 DHCP 服务器将黑客终端的 IP 地址 192.1.1.253 作为默认网关地址。如果终端选择通过 DHCP 自动配置网络信息方式,终端通过广播 DHCP 发现报文在以太网中寻找 DHCP 服务器,一旦某个终端选择伪造的 DHCP 服务器作为为其配置网络信息的 DHCP 服务器,将 IP 地址 192.1.1.253 作为默认网关地址,该终端所有传输给其他网络的 IP 分组首先发送给 IP 地址为 192.1.1.253 的黑客终端。

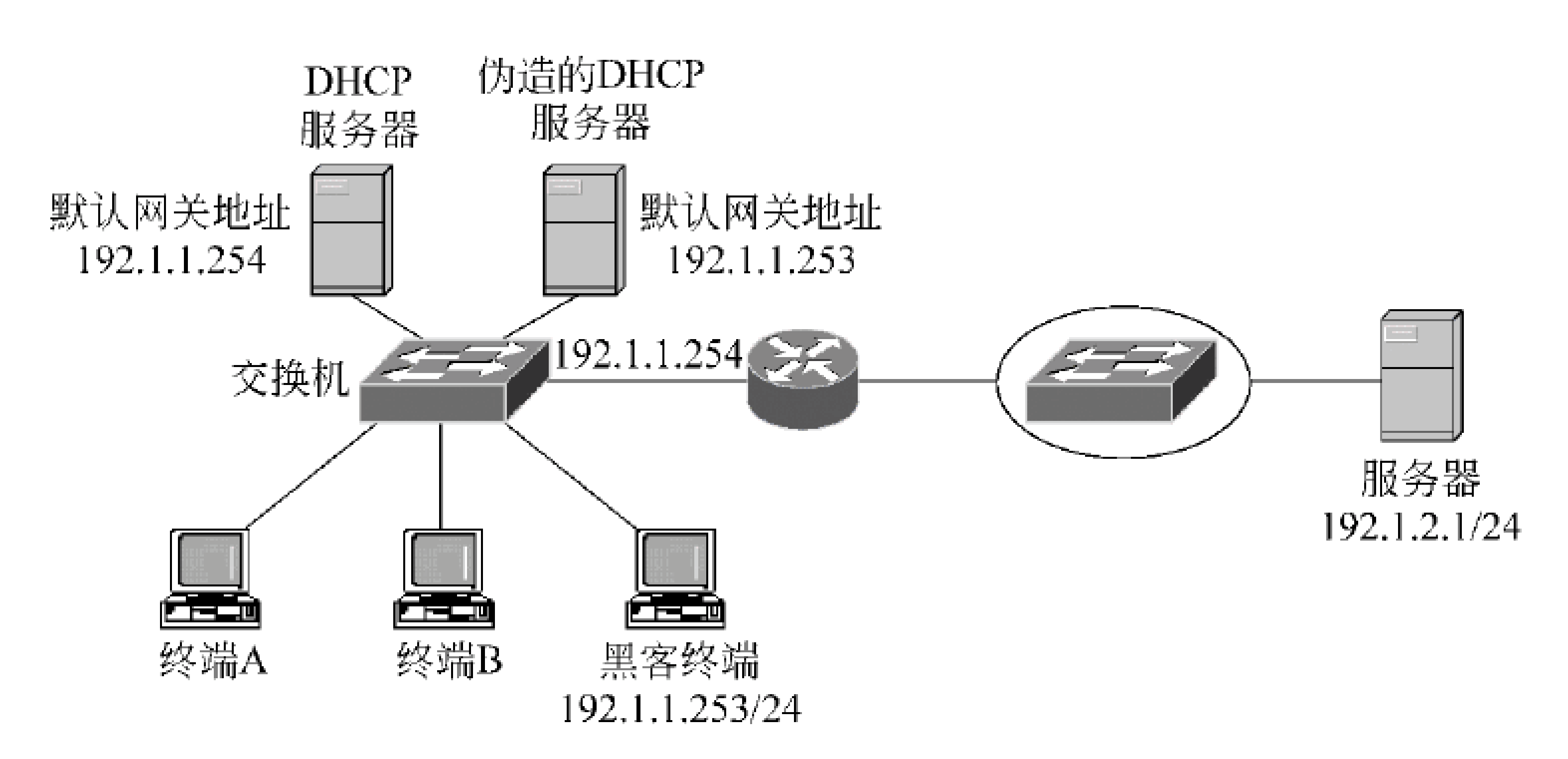


图 1.35 实施 DHCP 欺骗攻击网络结构

3. 实验步骤

(1) 启动 Packet Tracer,按照图 1.35 所示网络结构在逻辑工作区放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图 1.36 所示。

(2) 完成 Router0 接口 IP 地址和子网掩码配置,连接终端所在以太网的接口配置 IP 地址 192.1.1.254,该 IP 地址是所有终端及 DHCP 服务器的默认网关地址,将 hack 终端的 IP 地址和子网掩码配置为 192.1.1.253/24。

(3) 配置 DHCP 服务器,为作用域配置 IP 地址范围 192.1.1.1～192.1.1.30 和默认网关地址 192.1.1.254,配置界面如图 1.37 所示。配置伪造 DHCP 服务器,为作用域配置 IP 地址范围 192.1.1.1～192.1.1.30 和默认网关地址 192.1.1.253,将 hack 终端的

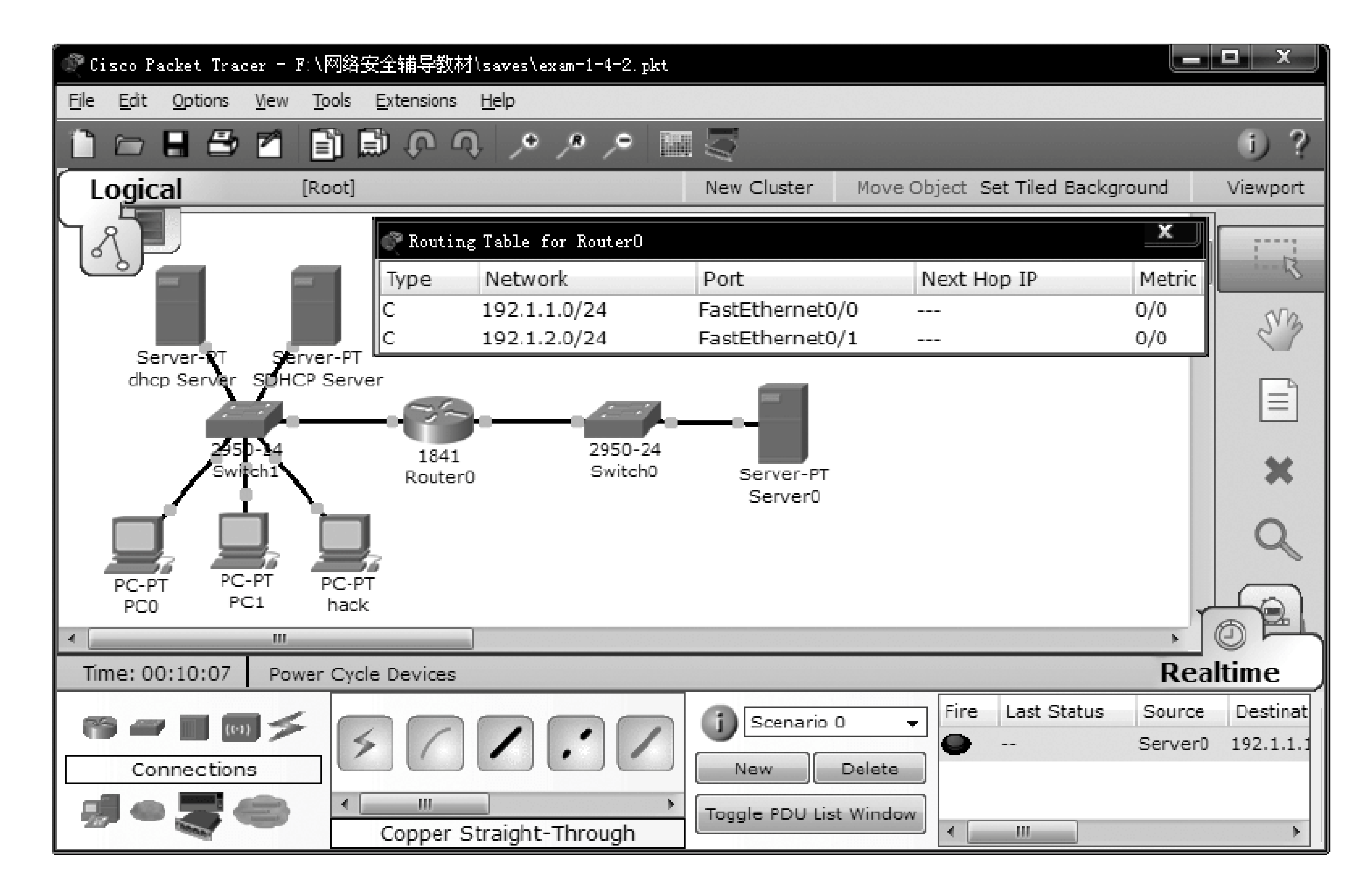


图 1.36　放置和连接设备后的逻辑工作区界面及路由表

IP 地址作为作用域的默认网关地址，配置界面如图 1.38 所示。

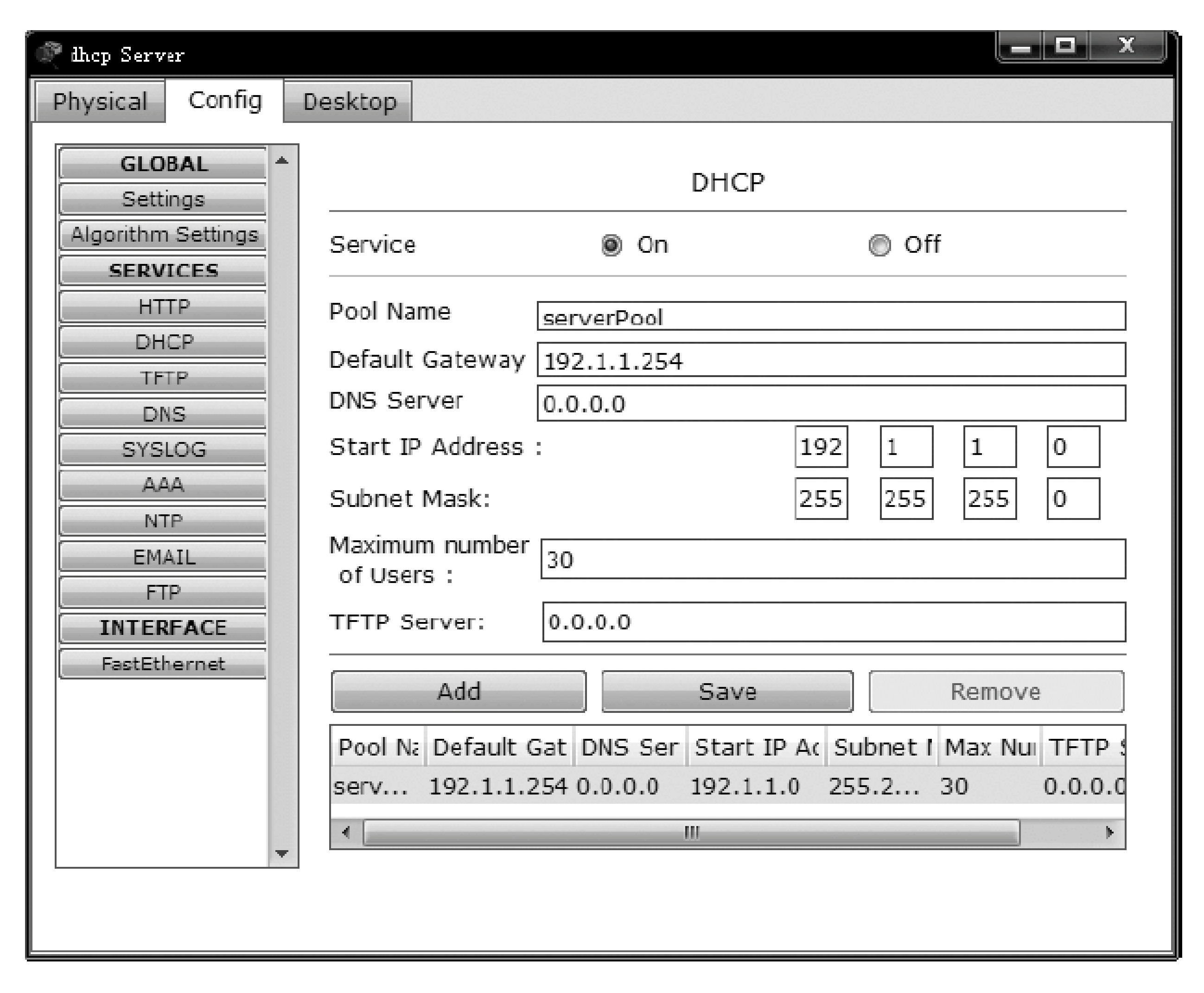


图 1.37　DHCP 服务器作用域配置界面

（4）启动终端 PC0 的配置界面，在 IP Configuration 选项组中选择 DHCP 单选按钮，终端 PC0 开始通过 DHCP 自动配置网络信息过程，这里 PC0 恰巧从伪造 DHCP 服务器获得网络配置信息，默认网关地址为 192.1.1.253，如图 1.39 所示。值得指出的是，为 PC0 配置网络信息的 DHCP 服务器是随机的，如果要求保证用伪造的 DHCP 服务器为终端配置网络信息，需要通过拒绝服务攻击使得 DHCP 服务器无法正常响应终端发送的 DHCP 发现和请求报文。

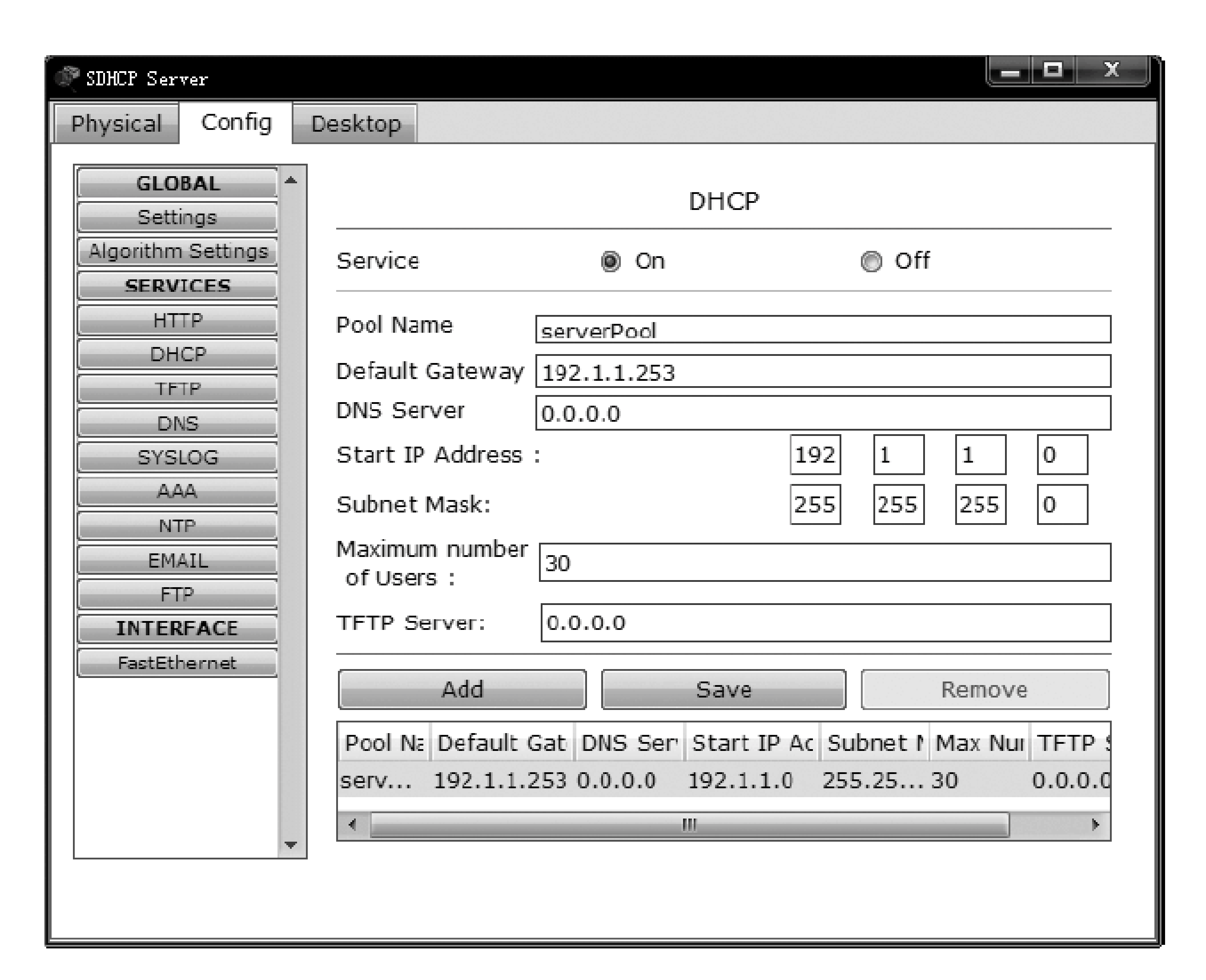


图 1.38 伪造的 DHCP 服务器作用域配置界面

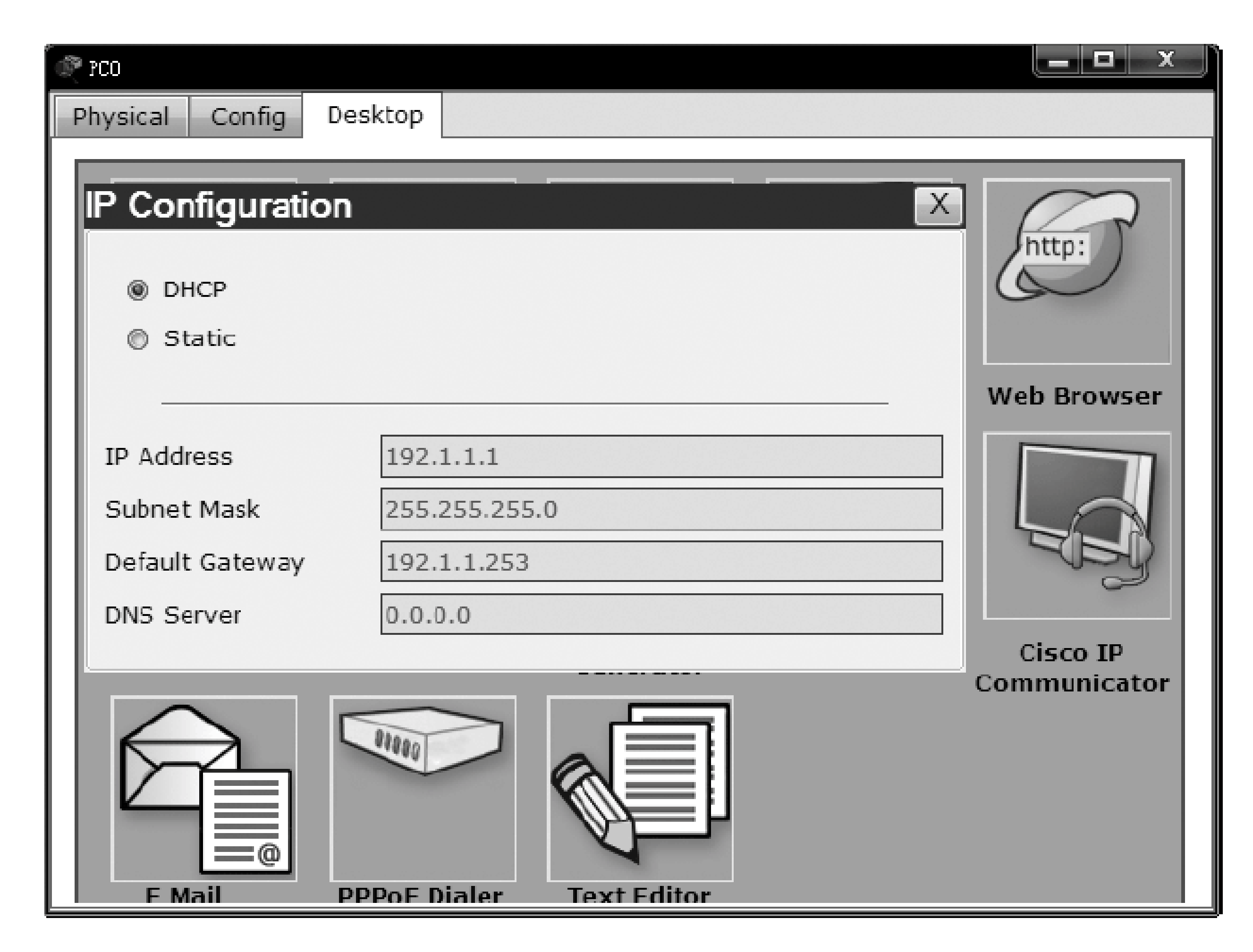


图 1.39 PC0 从伪造的 DHCP 服务器获得的网络配置信息

(5) PC0 创建并发送一个图 1.40 所示的以 Server0 的 IP 地址 192.1.2.1 为目的地址的 ICMP ECHO 请求报文，该 ICMP ECHO 请求报文被 PC0 首先发送给 hack 终端，如图 1.41 所示，hack 终端将截获所有 PC0 发送给其他网络中终端的 IP 分组。

1.4.6 DNS 欺骗攻击实验

1. 实验内容

(1) 完成 DHCP 服务器配置过程。

(2) 完成 DNS 服务器配置过程。

(3) 验证 DHCP 欺骗攻击机制。

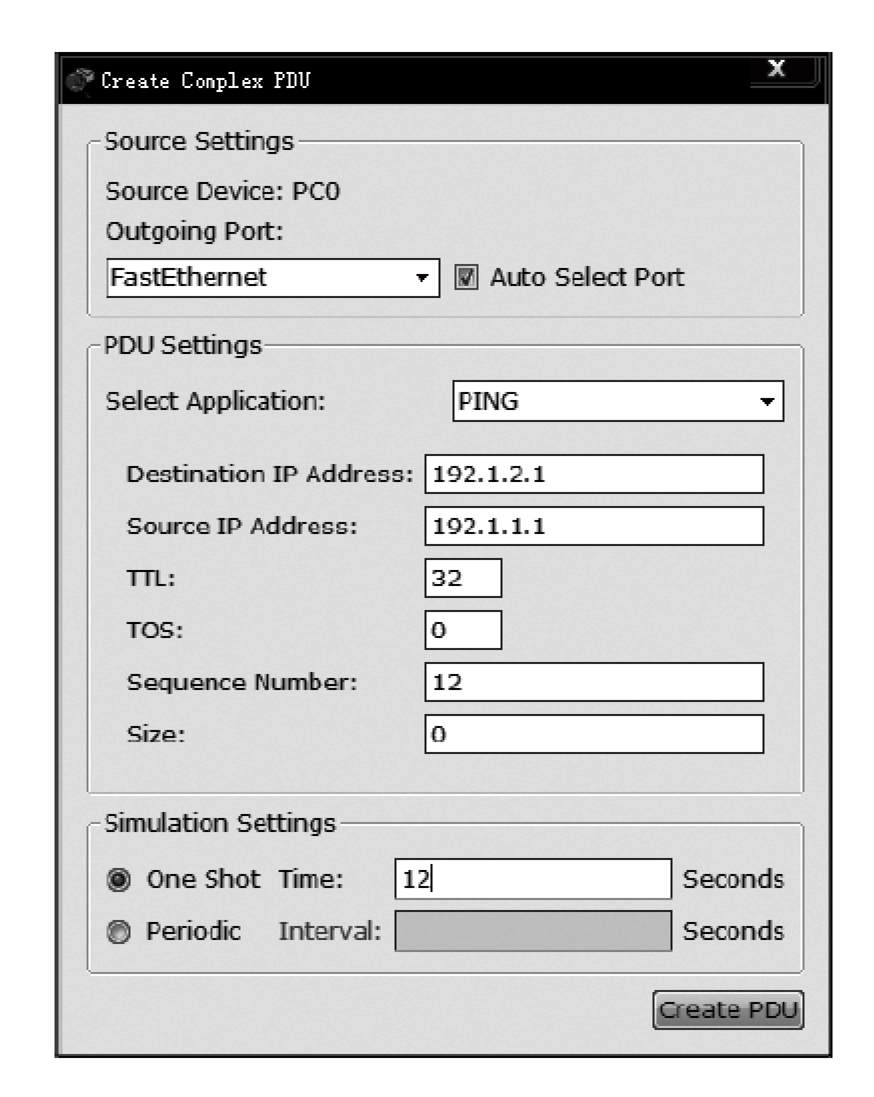


图 1.40　PC0 创建的 ICMP ECHO 请求报文

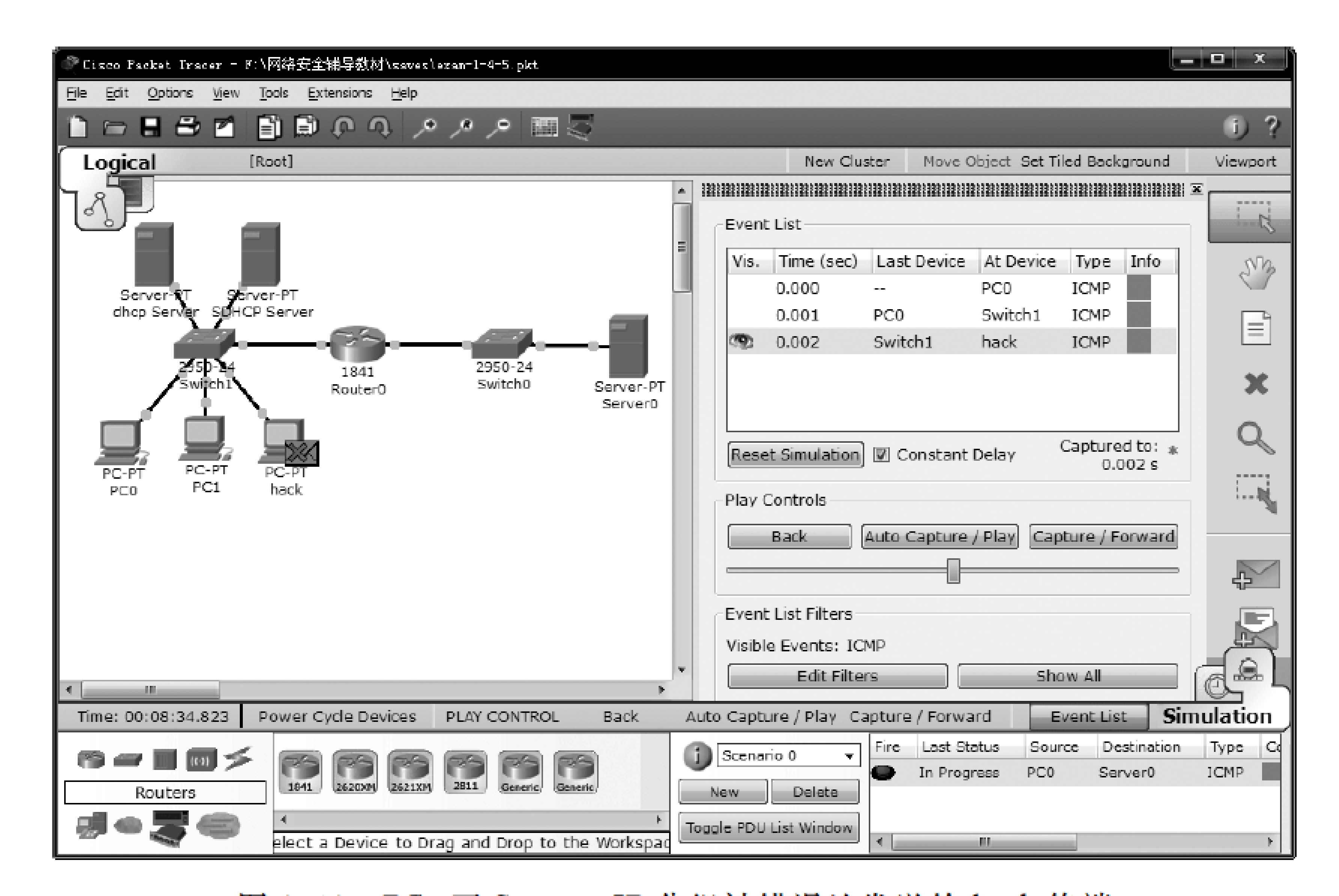


图 1.41　PC0 至 Server0 IP 分组被错误地发送给 hack 终端

(4) 验证 DNS 欺骗攻击机制。

(5)验证诱骗访问伪造 Web 网站过程。

2. 网络结构

网络结构如图 1.42 所示。黑客为了将用户对域名为 www.bank.com 的网站的访问诱骗到伪造的 Web 网站,伪造一个 DHCP 服务器,并将其接入以太网中,伪造的 DHCP 服务器将 DNS 服务器的 IP 地址设置为黑客伪造的 DNS 服务器的 IP 地址 192.1.2.1。在伪造的 DNS 服务器中,黑客将伪造的 Web 服务器 IP 地址 192.1.2.3 作为与域名

www.bank.com 绑定的 IP 地址。如果终端在自动配置网络信息过程中选择了伪造的 DHCP 服务器作为其配置网络信息的 DHCP 服务器，则伪造的 DNS 服务器地址 192.1.2.1 将作为本地 DNS 服务器地址。如果该终端在浏览器地址栏中输入 URL 为 http://www.bank.com，该终端将向伪造的 DNS 服务器发送一个请求将域名 www.bank.com 解析成 IP 地址的请求报文，伪造的 DNS 服务器将伪造的 Web 服务器地址 192.1.2.3 作为解析结果返回给该终端，该终端将访问伪造的 Web 服务器。如果在访问伪造的 Web 服务器过程中输入了银行卡卡号、密码等机密信息，后果不堪设想。

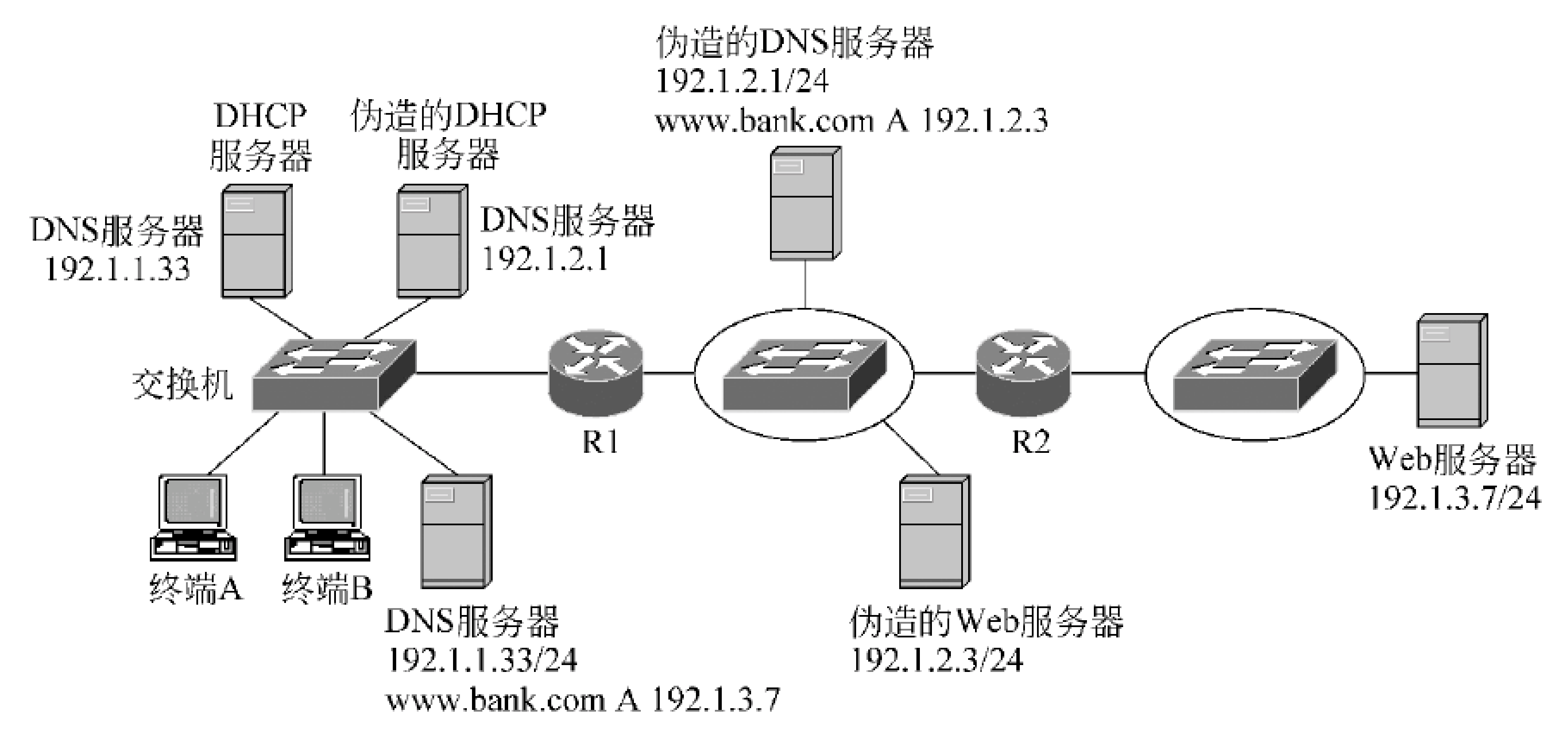


图 1.42　实施 DNS 欺骗攻击网络结构

3. 实验步骤

（1）启动 Packet Tracer，按照图 1.42 所示网络结构在逻辑工作区放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 1.43 所示。

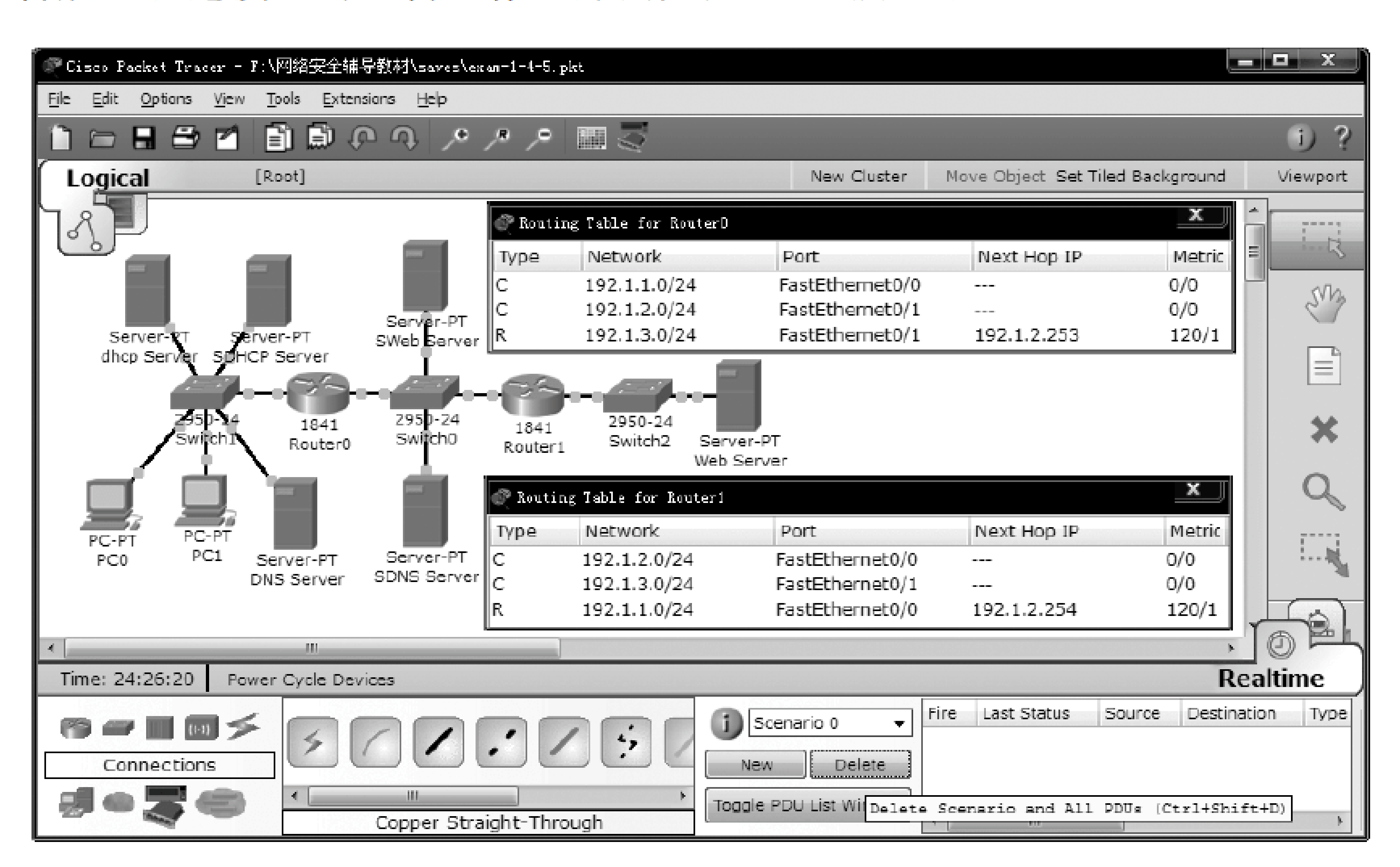


图 1.43　放置和连接设备后的逻辑工作区界面及路由表

(2) 按照图 1.42 所示网络配置信息配置路由器接口、各个终端和服务器的网络信息，在 Router0 和 Router1 启动 RIP，输入路由器直接连接的网络的网络地址，得到图 1.43 所示的 Router0 和 Router1 路由表。

(3) 配置 DHCP 服务器，为作用域配置 IP 地址范围 192.1.1.1～192.1.1.30、默认网关地址 192.1.1.254 和 DNS 服务器地址 192.1.1.33，配置界面如图 1.44 所示。配置伪造的 DHCP 服务器，为作用域配置 IP 地址范围 192.1.1.1～192.1.1.30、默认网关地址 192.1.1.254 和 DNS 服务器地址 192.1.2.1，将伪造的 DNS 服务器的 IP 地址作为作用域的 DNS 服务器地址，配置界面如图 1.45 所示。

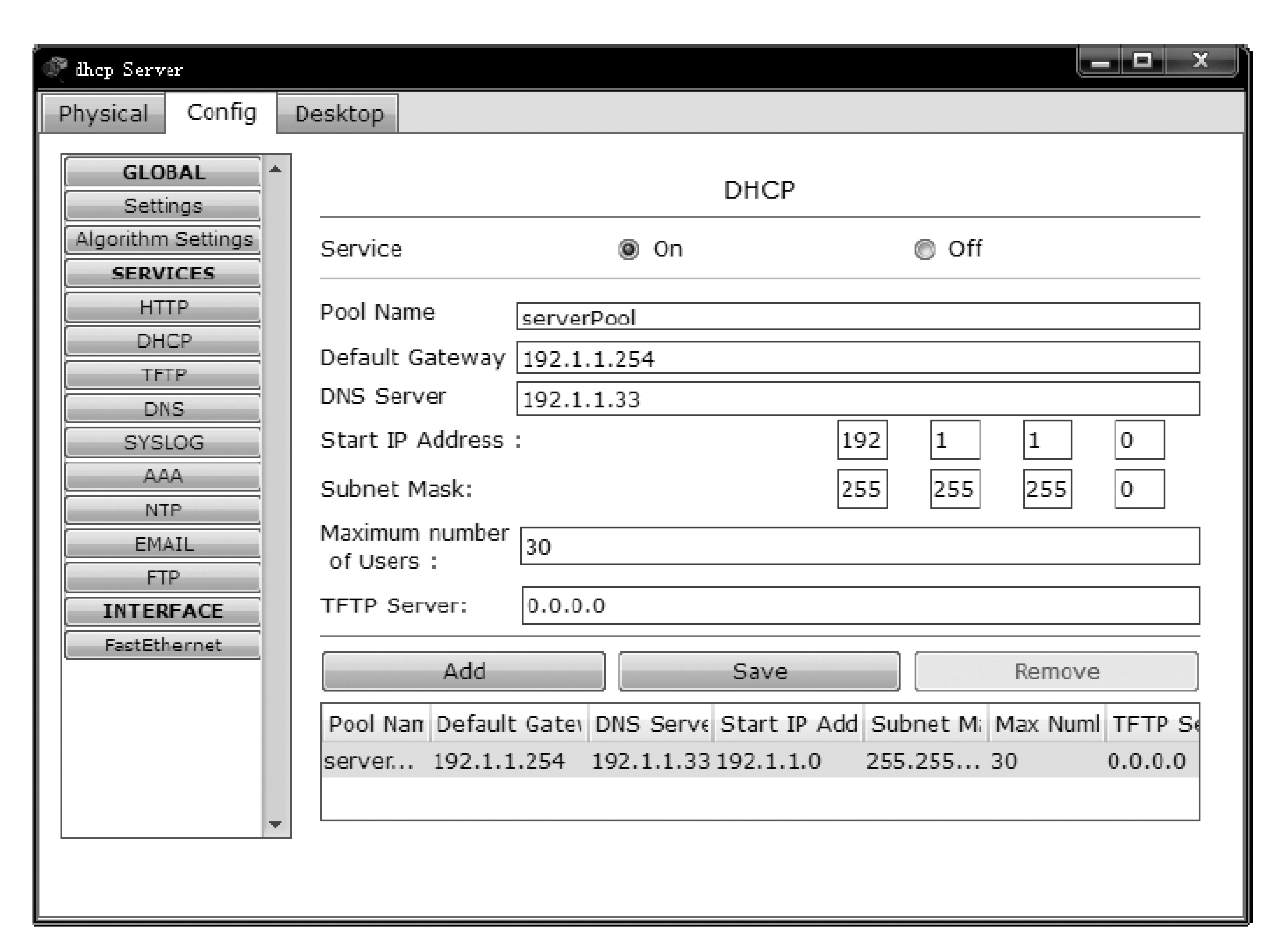


图 1.44　DHCP 服务器作用域配置界面

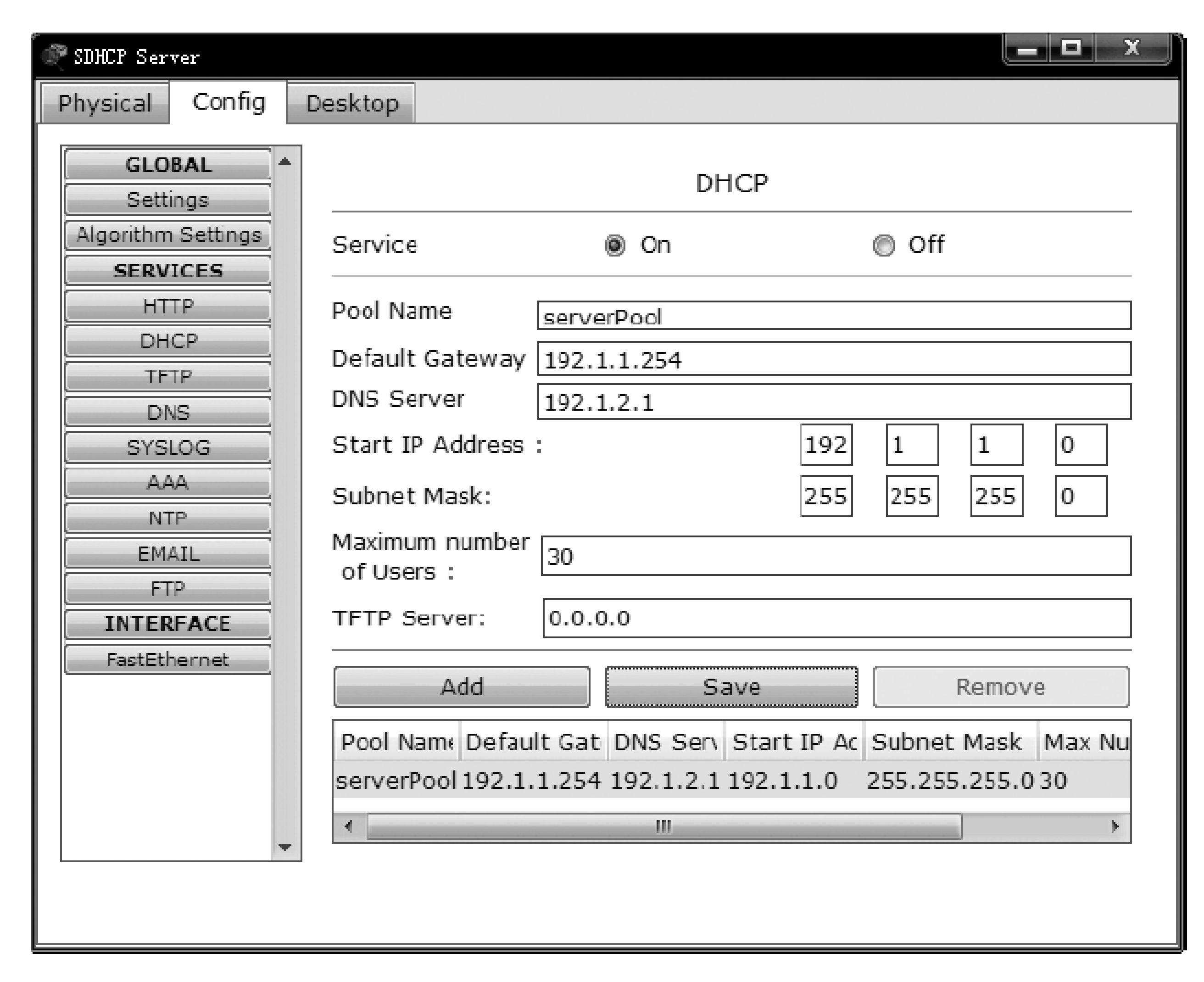


图 1.45　伪造的 DHCP 服务器作用域配置界面

(4) 配置 DNS 服务器,输入域名为 www.bank.com、类型为 A、IP 地址为 192.1.3.7 的资源记录,资源记录配置界面如图 1.46 所示。配置伪造的 DNS 服务器,输入域名为 www.bank.com、类型为 A、IP 地址为 192.1.2.3 的资源记录,将伪造的 Web 服务器的 IP 地址与域名 www.bank.com 绑定在一起,资源记录配置界面如图 1.47 所示。

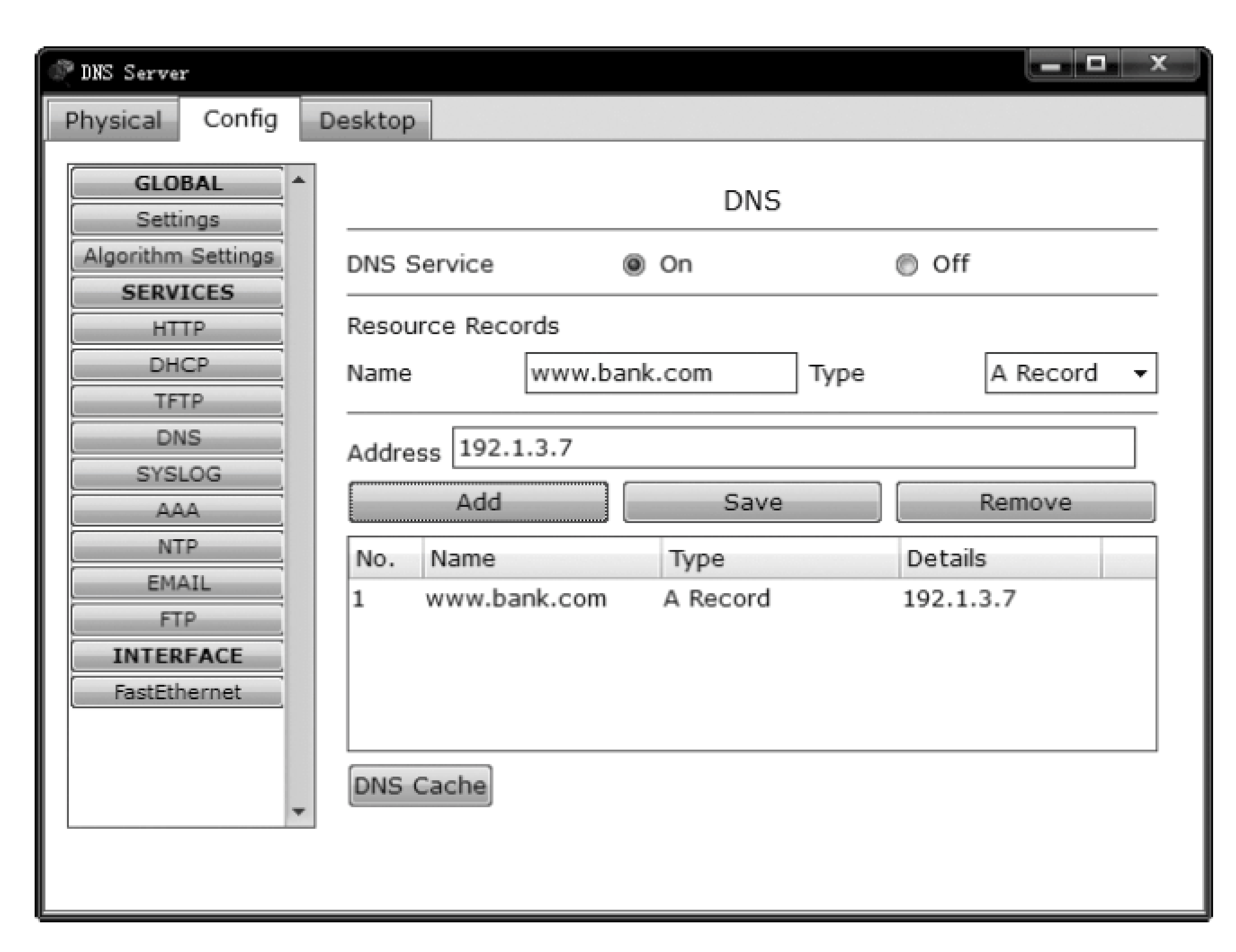


图 1.46 DNS 服务器资源记录配置界面

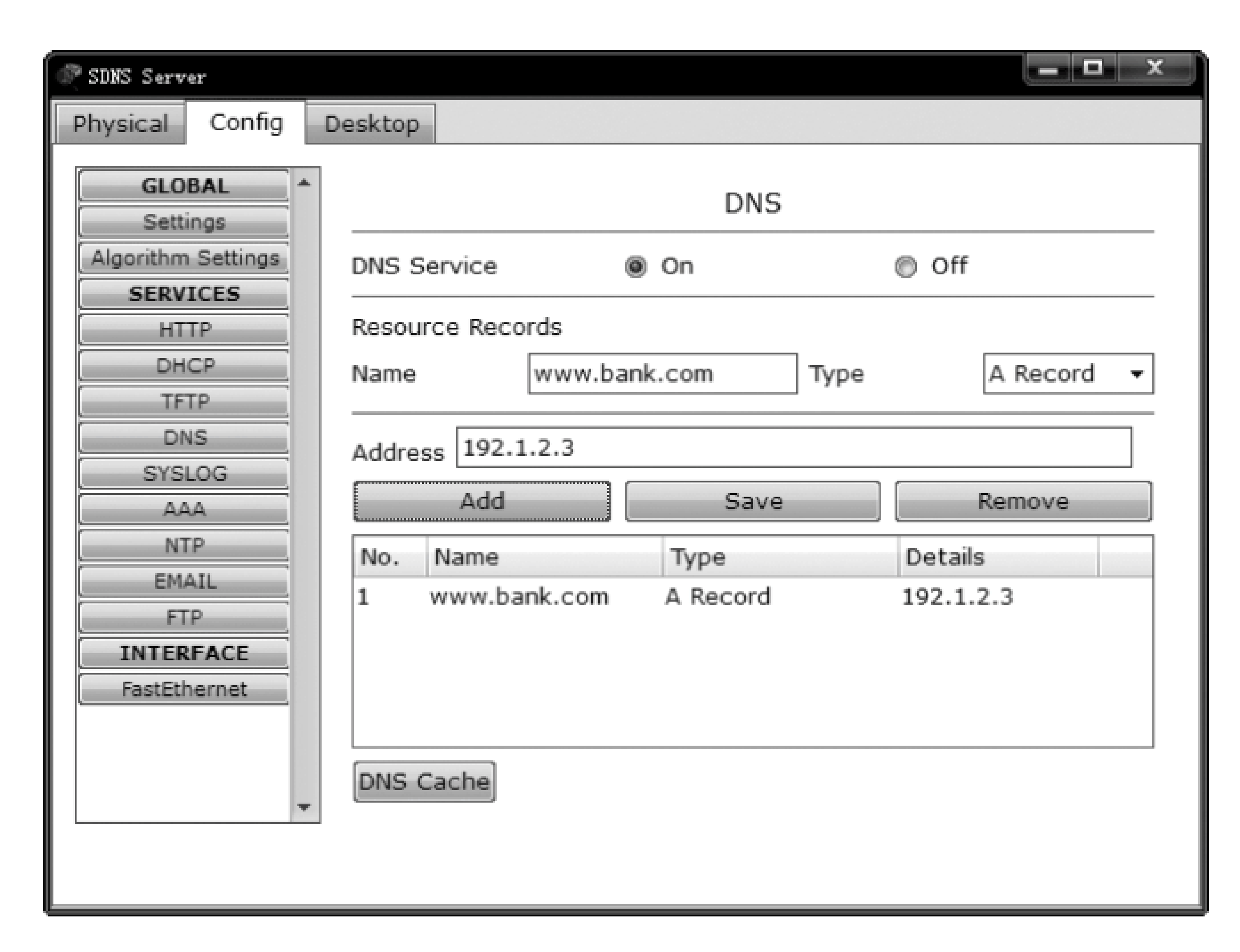


图 1.47 伪造的 DNS 服务器资源记录配置界面

(5) 启动 PC0 和 PC1 自动配置网络信息过程,假定 PC0 选择 DHCP 服务器为其配置网络信息,以 IP 地址 192.1.1.33 作为 DNS 服务器地址,如图 1.48 所示。PC1 选择伪造的 DHCP 服务器为其配置网络信息,以 IP 地址 192.1.2.1 作为 DNS 服务器地址,如图 1.49 所示。

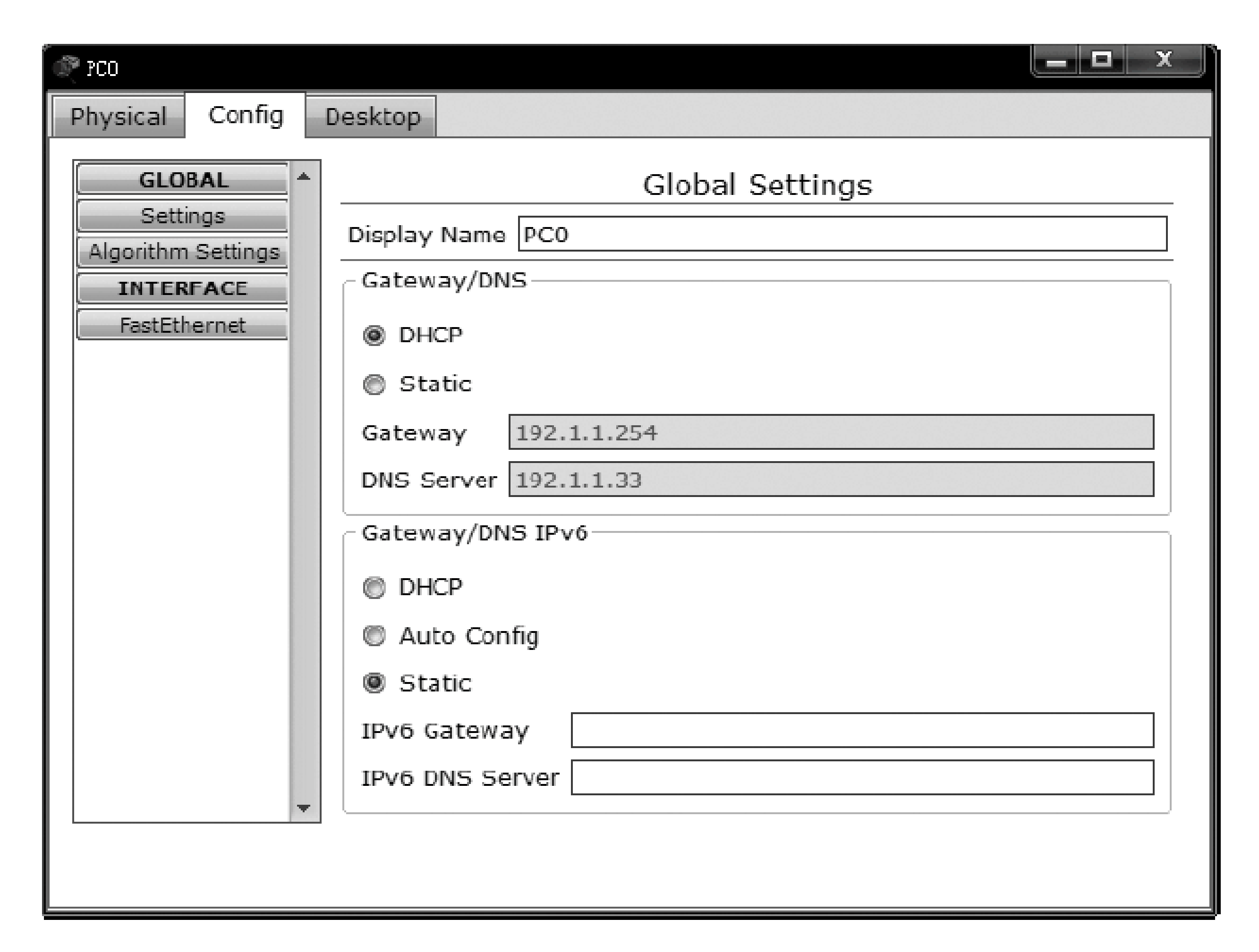


图 1.48　PC0 自动获得的 DNS 服务器地址

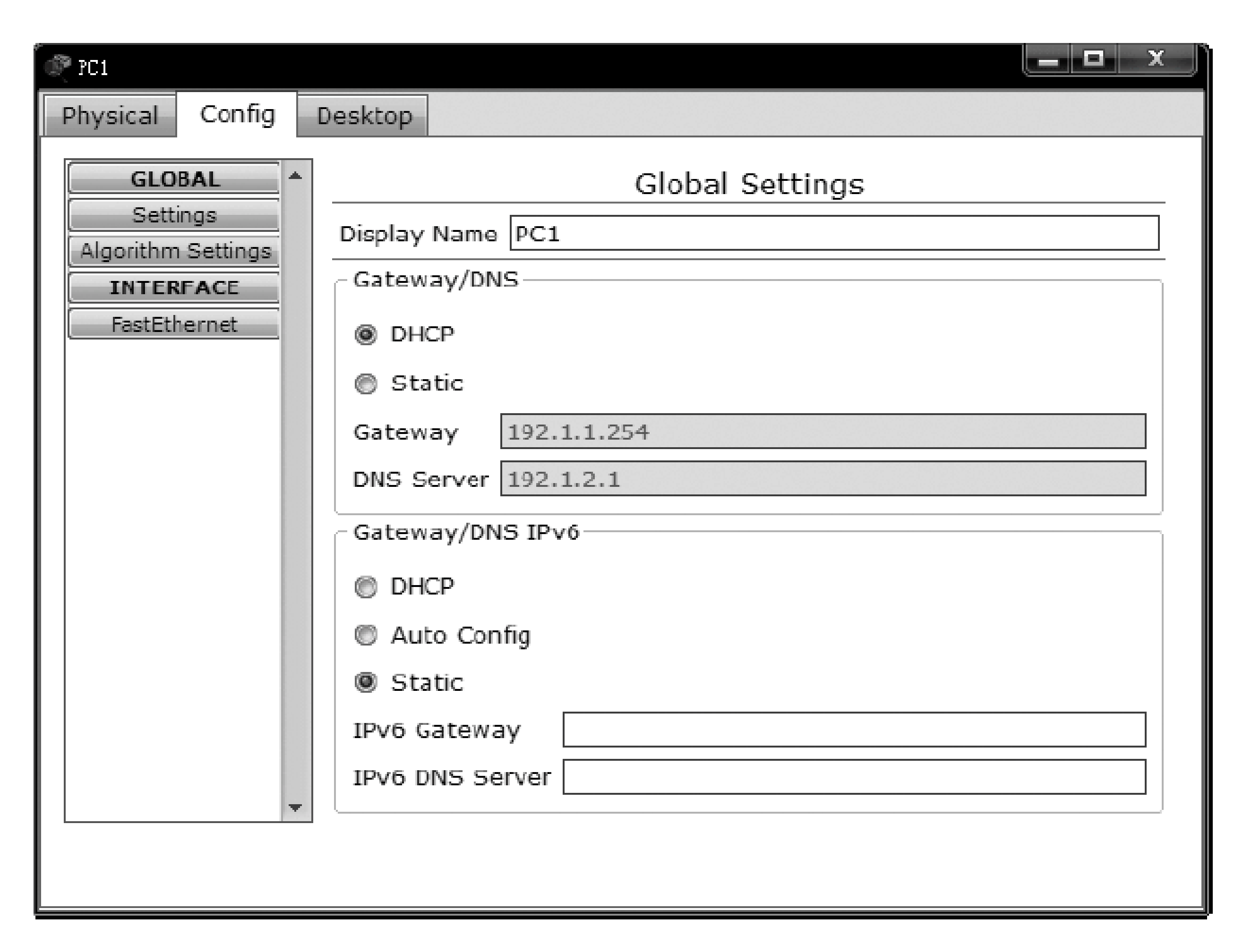


图 1.49　PC1 自动获得的伪造的 DNS 服务器地址

(6) 启动 PC0 实用程序 Browser，在地址栏输入 URL 为 http://www.bank.com，显示 Web 服务器主页，如图 1.50 所示。启动 PC1 实用程序 Browser，在地址栏输入 URL 为 http://www.bank.com，显示伪造的 Web 服务器主页，如图 1.51 所示。伪造的 Web 服务器主页首行是 forged web server。

1.4.7　非法接入实验

1. 实验内容

(1) 验证接入控制过程。

(2) 配置安全端口。

(3) 验证安全端口的缺陷。

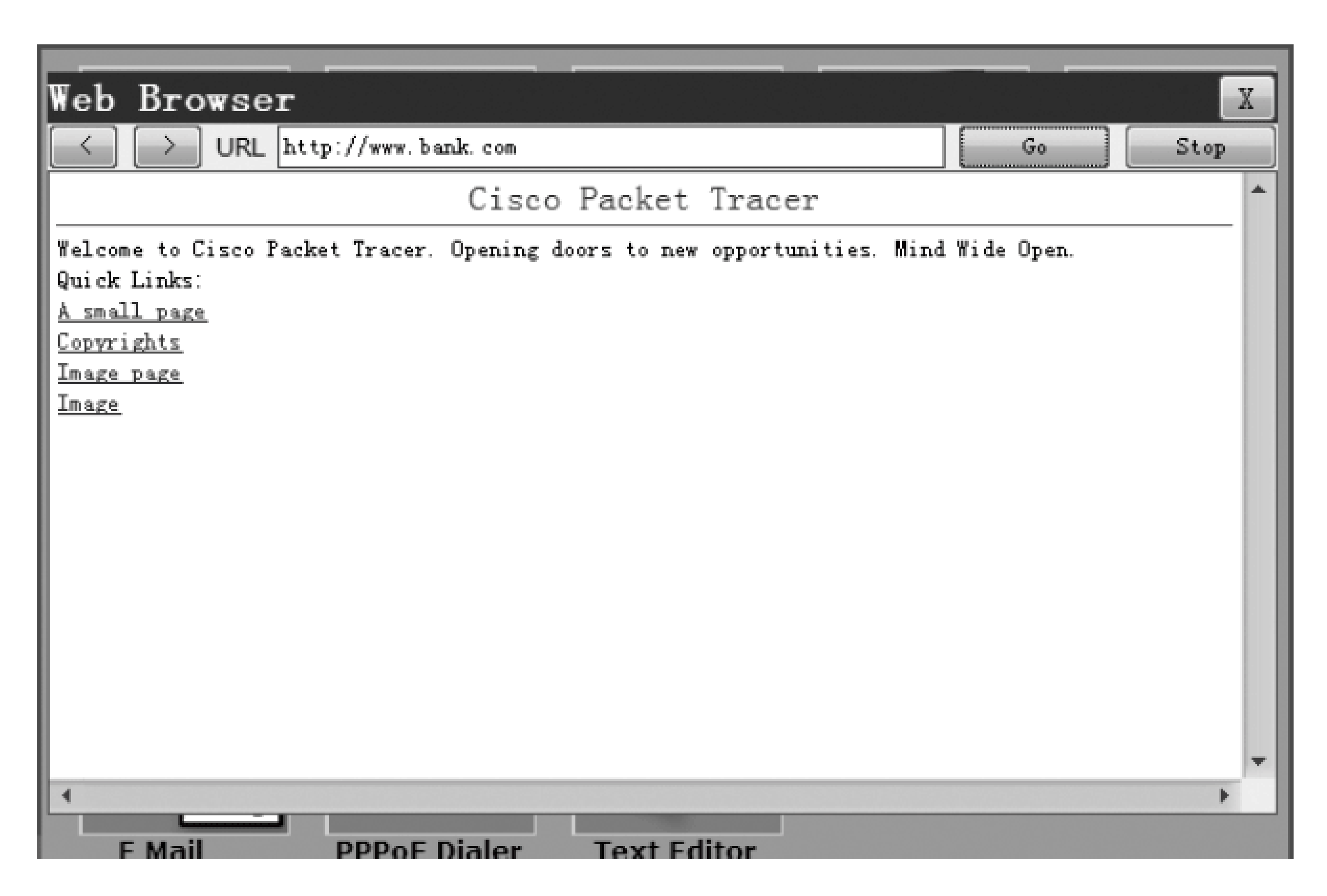


图 1.50 PC0 访问到的 Web 服务器主页

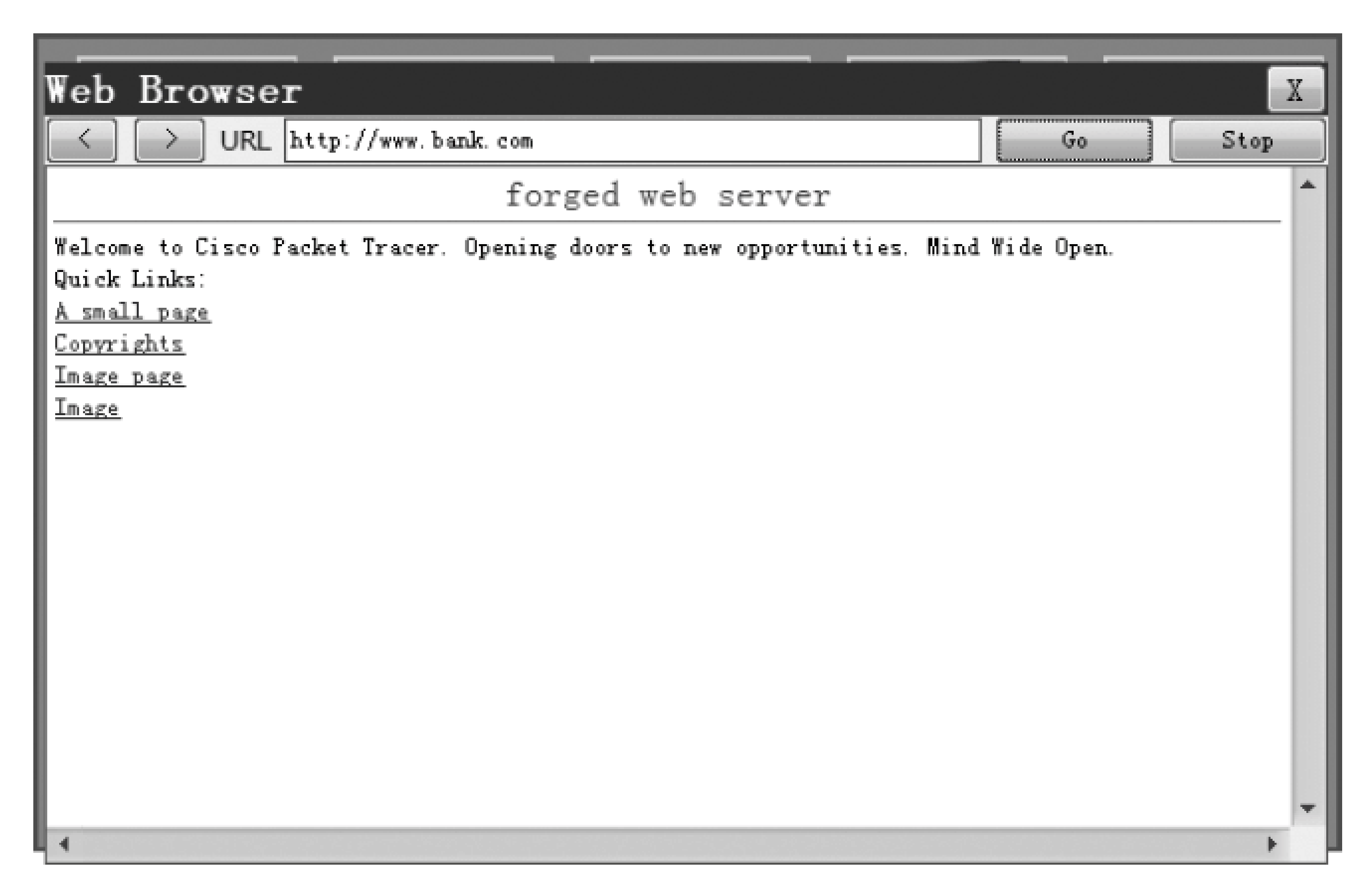


图 1.51 PC1 访问到的伪造的 Web 服务器主页

2. 网络结构

网络结构如图 1.52 所示。交换机端口 1 配置为安全端口，只允许接收源 MAC 地址为 MAC A 的 MAC 帧，这样配置的目的是只允许终端 A 接入交换机端口 1。如果黑客能够在交换机端口 1 和终端 A 之间插入一台集线器，并将黑客终端接入集线器，这样，一是可以嗅探终端 A 和交换机之间传输的 MAC 帧，并因此获得终端 A 的 MAC 地址 MAC A；二是通过将自身 MAC 地址改为 MAC A 而非法接入交换机端口 1。

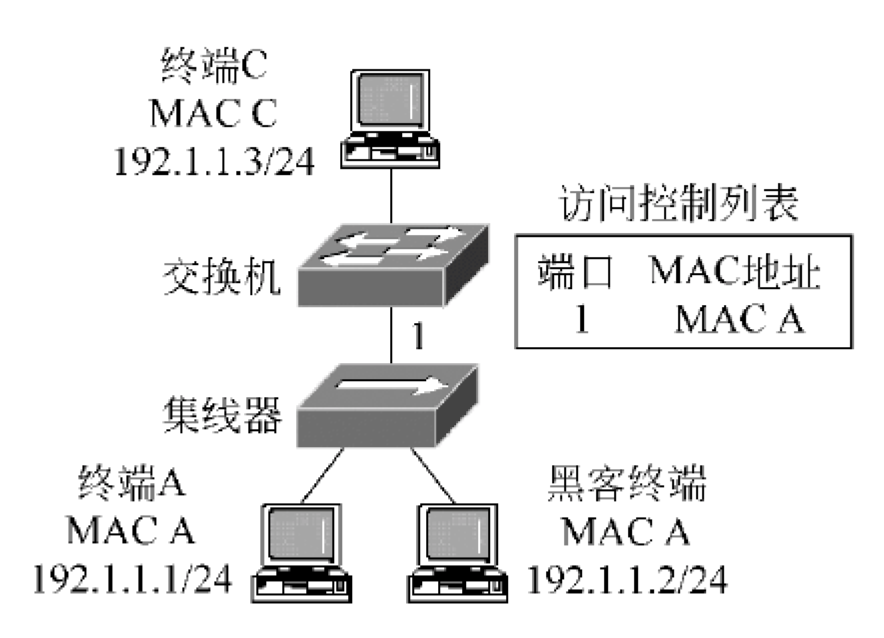


图 1.52 实施非法接入网络结构

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区放置

交换机和终端，将 PC2 接入交换机端口 FastEthernet0/2，通过命令行配置过程将交换机端口 FastEthernet0/1 配置为安全端口，MAC 地址设置为 PC0 的 MAC 地址 000C.8564.BB10，将 PC0 接入交换机端口 FastEthernet0/1，完成设备放置和连接后的逻辑工作区界面如图 1.53 所示。通过 Ping 操作验证 PC0 和 PC2 之间的连通性。

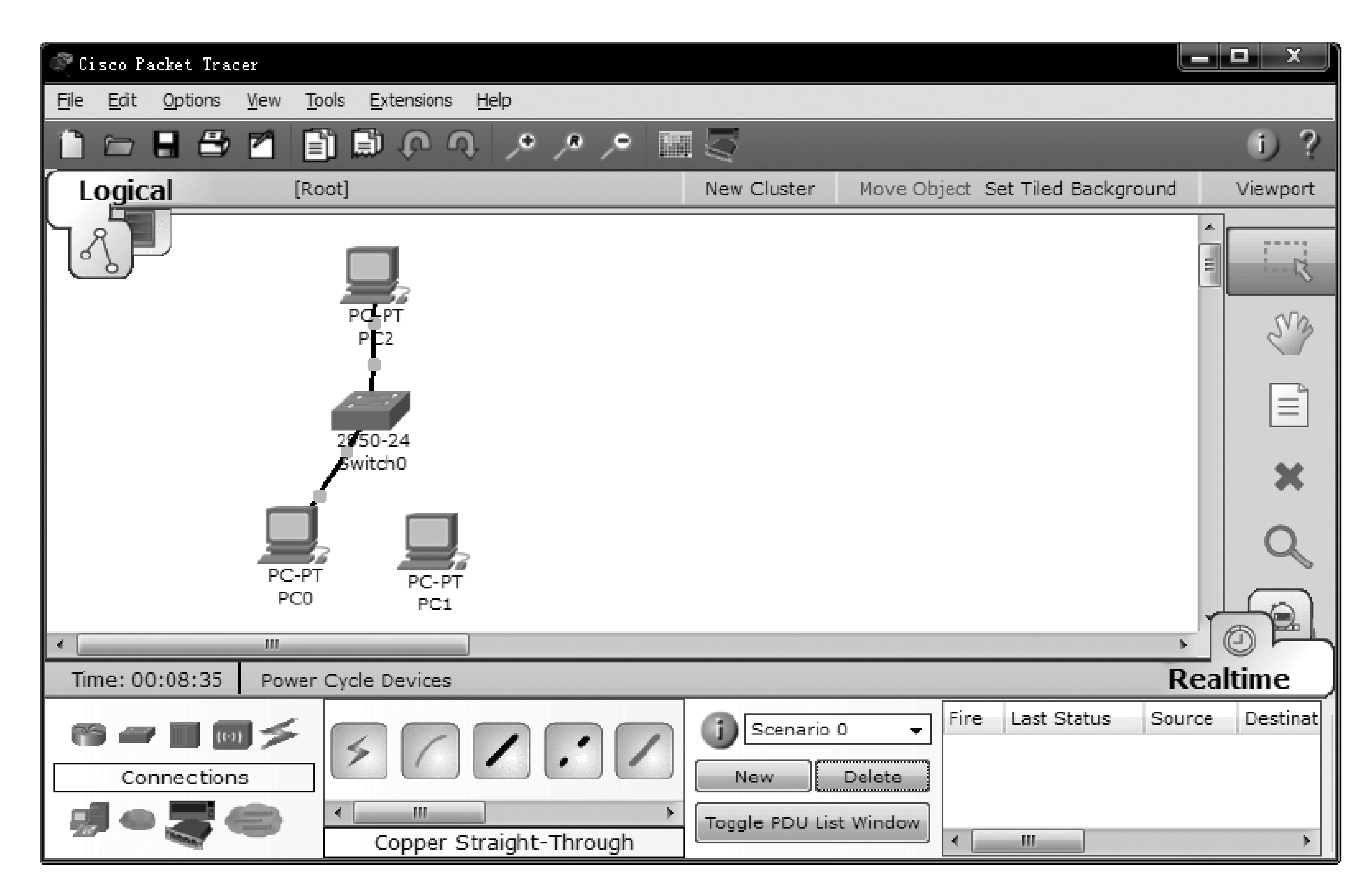


图 1.53　PC0 和 PC2 之间正常通信

(2) 删除交换机端口 FastEthernet0/1 和 PC0 之间的直连双绞线，将 PC1 接入交换机端口 FastEthernet0/1，通过 Ping 操作验证 PC1 和 PC2 之间的连通性，可以发现交换机端口 FastEthernet0/1 关闭，如图 1.54 所示。

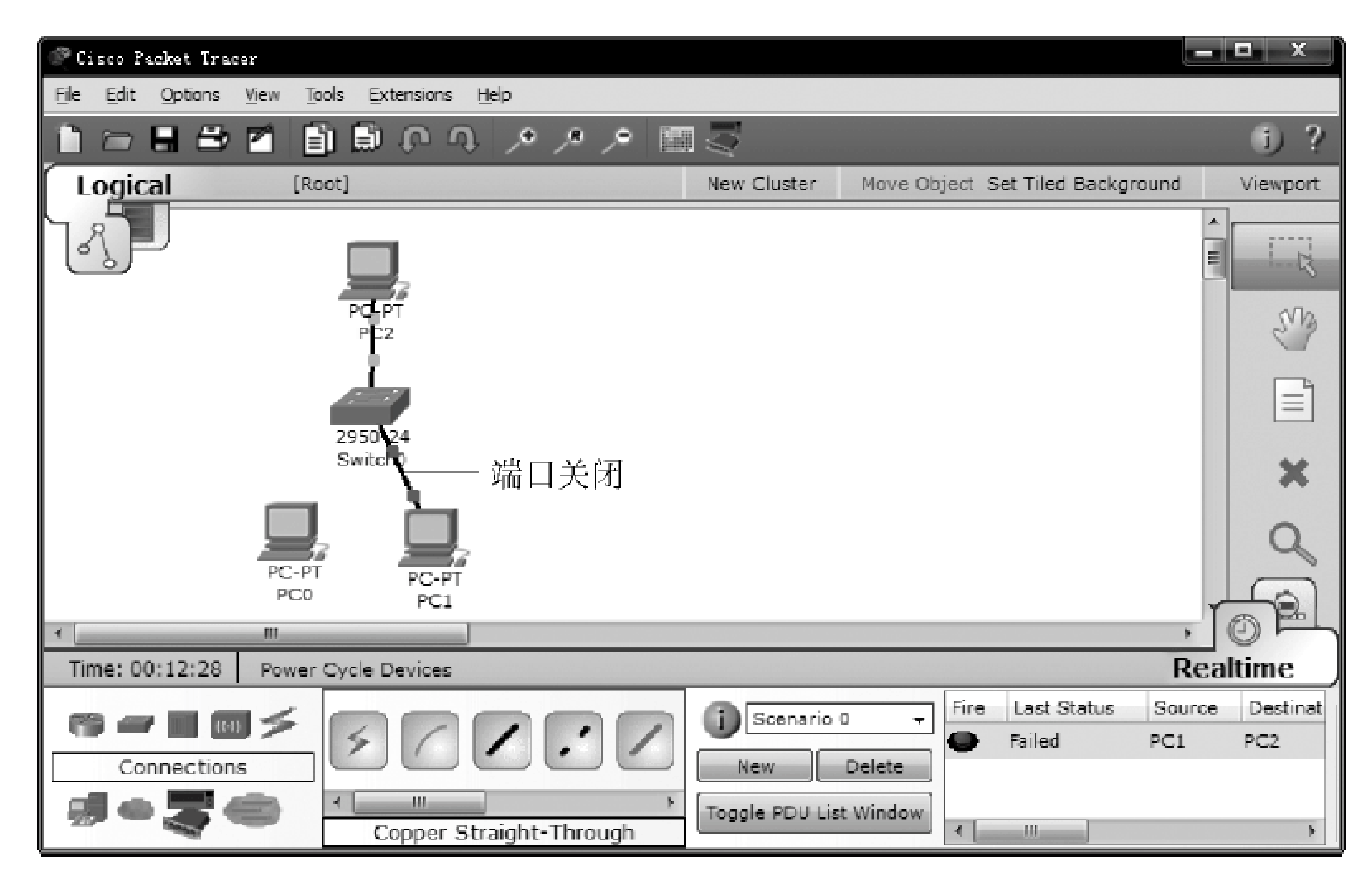


图 1.54　交换机端口 FastEthernet0/1 关闭

(3) 通过命令 shutdown 和 no shutdown 重新打开交换机端口 FastEthernet0/1，按

照图 1.52 所示网络结构放置和连接网络设备,放置和连接网络设备后的逻辑工作区界面如图 1.55 所示。将 PC1 的 MAC 地址改为 PC0 的 MAC 地址 000C.8564.BB10,通过 Ping 操作验证终端之间连通性,发现 PC1 和 PC0 可以同时和网络中的其他终端通信,PC1 成功实现非法接入。

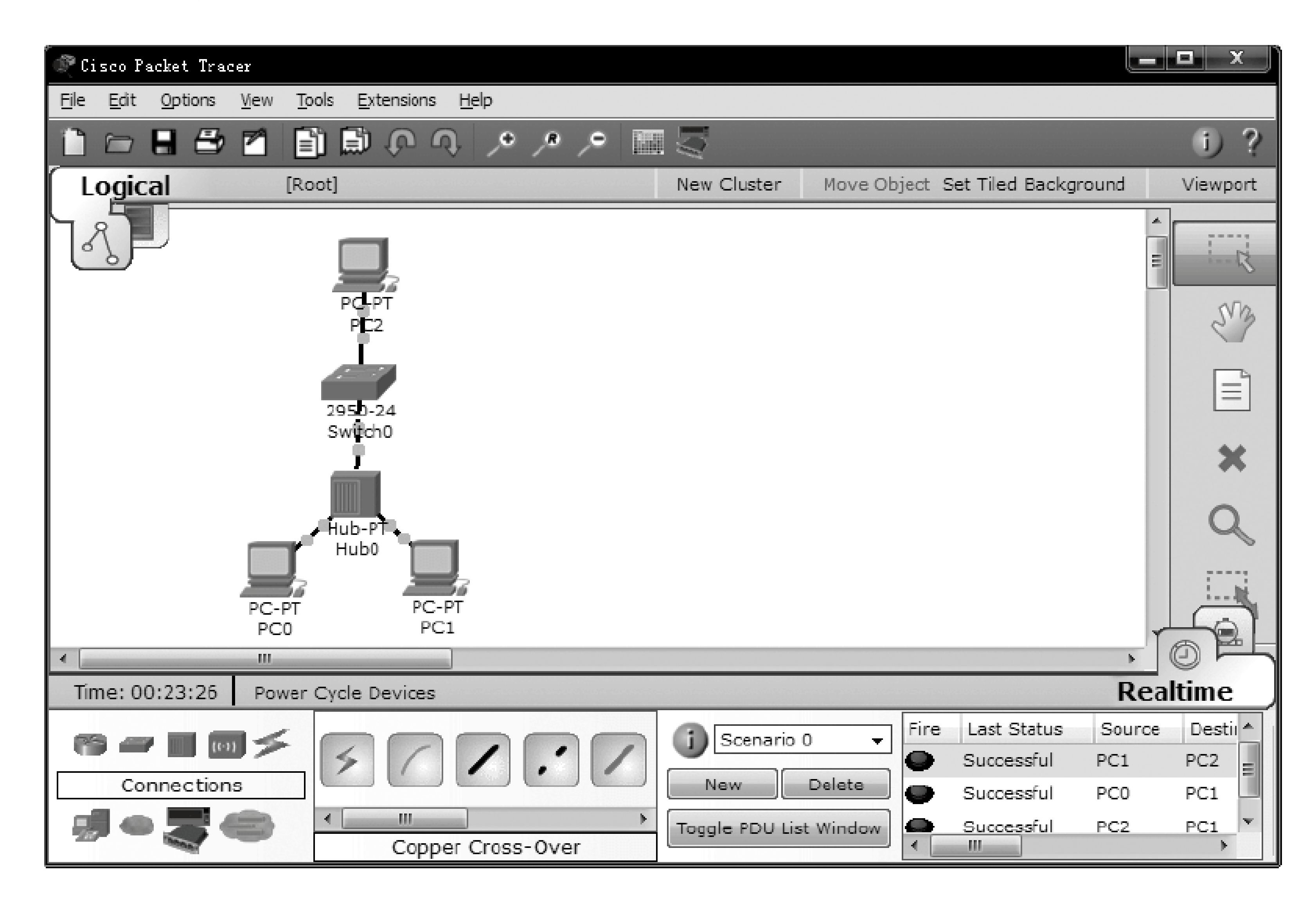


图 1.55 放置和连接设备后的逻辑工作区界面

4. 交换机命令行配置过程

```
Switch>enable
Switch#configure terminal
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode access
                                    (将端口配置为接入端口)
Switch(config-if)#switchport port-security
                                    (启动安全端口功能)
Switch(config-if)#switchport port-security maximum 1
                                    (将访问控制列表中的 MAC 地址数上限配置为 1)
Switch(config-if)#switchport port-security mac-address 000C.8564.BB10
                                    (只允许接入 MAC 地址为 000C.8564.BB10 的终端)
Switch(config-if)#exit
```

第2章 恶意代码分析与防御

CHAPTER

2.1 知识要点

2.1.1 病毒传播和感染方式

1. 病毒传播方式

这里的病毒是指狭义病毒，是一种必须嵌入在宿主程序中，具有自我复制能力（感染）的恶意代码，不包括蠕虫，蠕虫属于广义病毒，具有通过网络自动传播、自动激活特性。狭义病毒必须借助人力实现传播。

（1）移动存储媒介。

将一台主机系统中感染病毒的宿主程序复制到移动存储媒介，然后通过移动存储媒介将该宿主程序复制到另一台主机系统中，并运行该宿主程序。

（2）邮件。

接收一个附件是感染病毒的宿主程序的邮件，并打开附件。由于邮件正文可以包含脚本，如果脚本就是一段具有病毒特征的恶意代码，打开邮件正文即激活病毒。

（3）Web 主页。

由于网页中可以包含脚本，如果脚本就是一段具有病毒特征的恶意代码，浏览网页即激活病毒。由于浏览器需要将作为恶意代码的脚本从 Web 服务器下载到本地执行，因此将这样的脚本称为恶意移动代码。

（4）下载实用程序。

网站提供大量免费下载的实用程序，这些实用程序可能就是感染病毒的宿主程序，一旦运行该实用程序将会激活病毒。

2. 病毒激活方式

首次激活病毒必须运行宿主程序，如打开邮件附件、浏览包含脚本的 Web 主页、运行下载的实用程序等。一旦激活病毒，病毒感染主机系统，感染方式和病毒的再次激活方式有关。

（1）感染可执行文件。

病毒感染可执行文件就是将自身嵌入到某个可执行文件中，一旦运行该可执行文件将激活病毒。

（2）感染引导扇区。

引导扇区中存放着引导程序，BIOS中的自检程序完成硬件系统检测后，将引导扇区中的引导程序读入内存，并由引导程序完成操作系统的启动过程。如果病毒首次激活后感染引导程序，则每一次启动主机系统都将激活病毒。

（3）感染中断处理程序。

如果病毒首次激活后感染中断处理程序，如鼠标中断处理程序，由于每一次鼠标操作都将执行鼠标中断处理程序，意味着每一次鼠标操作都将激活病毒。

（4）感染文档文件。

Office文档可以感染宏病毒，一旦打开感染宏病毒的Office文档将激活病毒。

（5）修改注册表。

如果病毒首次激活时只感染可执行文件，则必须手工运行该可执行文件才能再次激活病毒。一般情况下，为了实现自动激活，在感染某个可执行文件后，通过修改注册表将该可执行文件添加到自启动项列表中，由于操作系统完成启动过程将自动执行自启动项列表中包含的可执行文件，因此每一次启动操作系统都将激活病毒。

3．蠕虫传播方式

蠕虫和狭义病毒的最大区别在于：一是蠕虫只通过网络传播；二是蠕虫利用主机系统漏洞实现自动传播和自动激活；三是蠕虫入侵某个主机系统后，能够自动选择新的攻击对象，开始新一轮的攻击；四是蠕虫入侵某个主机系统后不一定感染宿主程序。某个黑客主机一旦激活蠕虫，蠕虫实施以下攻击过程。

（1）选择攻击对象。可以人工配置攻击对象列表，也可以从黑客主机存放的地址信息中（如邮件地址表）选择攻击对象。

（2）扫描攻击对象。通过扫描发现攻击对象的漏洞。

（3）渗入攻击对象。发现攻击对象漏洞后，利用漏洞上传引导程序，引导程序的作用是完成入侵准备工作，如建立具有管理员权限的账户、建立与黑客主机的反向连接等。

（4）入侵。利用引导程序完成蠕虫的上传，并激活蠕虫，一旦在攻击对象激活蠕虫，攻击对象成为新的黑客主机，自动开始过程（1）～（4）的新一轮攻击。

（5）黑客主机除了进行（1）～（4）的攻击过程外，同时将蠕虫作为邮件附件发送给邮件地址表中包含的所有信箱，一旦接收到邮件的用户打开邮件附件将激活蠕虫。如果入侵的主机系统是一个Web服务器，将蠕虫以恶意移动代码的形式嵌入Web主页中，一旦某个用户的浏览器访问了该Web主页也将激活蠕虫。所有激活蠕虫的主机系统都成为新的黑客主机，自动开始新一轮的攻击，这是蠕虫得以快速传播的主要原因。

2.1.2 恶意代码危害

1．破坏主机系统

在满足激发破坏操作的条件时，恶意代码将删除系统中的文件，重新格式化硬盘，使

主机系统崩溃。

2. 实现非法访问

恶意代码激活后，往往建立黑客实现非法访问的通路，如创建具有管理员权限的账户、安装木马客户端、打开一些服务(如 Telnet 服务)等，为黑客以后非法访问该主机系统提供便利。随着信息资源的重要性日益增强，非法访问的危害性越来越大。目前大量的恶意代码都以实现非法访问为目的。

3. 传播病毒和蠕虫

一旦激活病毒，病毒除了感染主机系统中的文件外，还会将感染病毒的宿主程序作为邮件附件发送给邮件地址表中包含的所有信箱，引发病毒的进一步传播。蠕虫的自动传播和自动激活功能使蠕虫可以在网络中更加快速蔓延。

4. 实施拒绝服务攻击

破坏主机系统就是一种通过破坏主机系统的可用性而实现的拒绝服务攻击，恶意代码除此以外，可以通过向某个攻击目标发送大量的 ICMP ECHO 请求或响应报文，消耗掉该攻击目标连接网络的链路的带宽和该攻击目标的处理能力，使其无法和其他主机系统正常通信。另外，大量激活恶意代码的主机系统通过同步行动可以瘫痪掉任何服务器和转发结点(如路由器)、消耗掉任何关键链路的带宽，使网络无法正常提供服务。

2.1.3　网络安全技术对阻止病毒和蠕虫传播的作用

1. NAT 弱安全功能

(1) NAT 隐藏内部网络。

NAT(Network Address Translation，网络地址转换)的功能有两个：一是隐藏内部网络，二是允许内部网络分配与外部网络相同的全球 IP 地址。隐藏内部网络原理如图 2.1 所示。对于外部网络终端，分配本地 IP 地址的内部网络是透明的，因此路由器 R2 的路由表中不存在用于指明通往目的网络 192.168.1.0/24 传输路径的路由项。如果路由器 R2 接收到以属于网络 192.168.1.0/24 的 IP 地址为目的地址的 IP 分组，将丢弃这样的 IP 分组，这就保证外部网络终端无法对内部网络终端实施漏洞扫描和入侵。如果内部网络终端需要访问外部网络中的资源，必须由内部网络终端发起资源访问过程，当路由器 R1 接收到内部网络终端用于发起访问外部网络中资源的第一个 IP 分组时，建立内部网络本地 IP 地址和全球 IP 地址池 1(网络地址 193.1.1.16/28)中某个全球 IP 地址之间的绑定关系，以后所有由该内部网络终端发送的和该次资源访问过程有关的 IP 分组经路由器 R1 转发后，IP 分组的源 IP 地址由内部网络终端的本地 IP 地址变为与该本地 IP 地址绑定的全球 IP 地址。同样，外部网络终端发送给该内部网络终端的 IP 分组以该全球 IP 地址为目的 IP 地址，这样的 IP 分组经路由器 R1 转发后，IP 分组的目的 IP 地址变为与该全球 IP 地址绑定的内部网络终端的本地 IP 地址。因此，路由器 R2 的路由表中需要给出用于指明通往网络 193.1.1.16/28 的传输路径的路由项，但在建立内部网络本地 IP 地址与某个全球 IP 地址之间绑定关系之前，外部网络终端无法通过全球 IP 地址池 1 中的全球 IP 地址与内部网络终端通信。

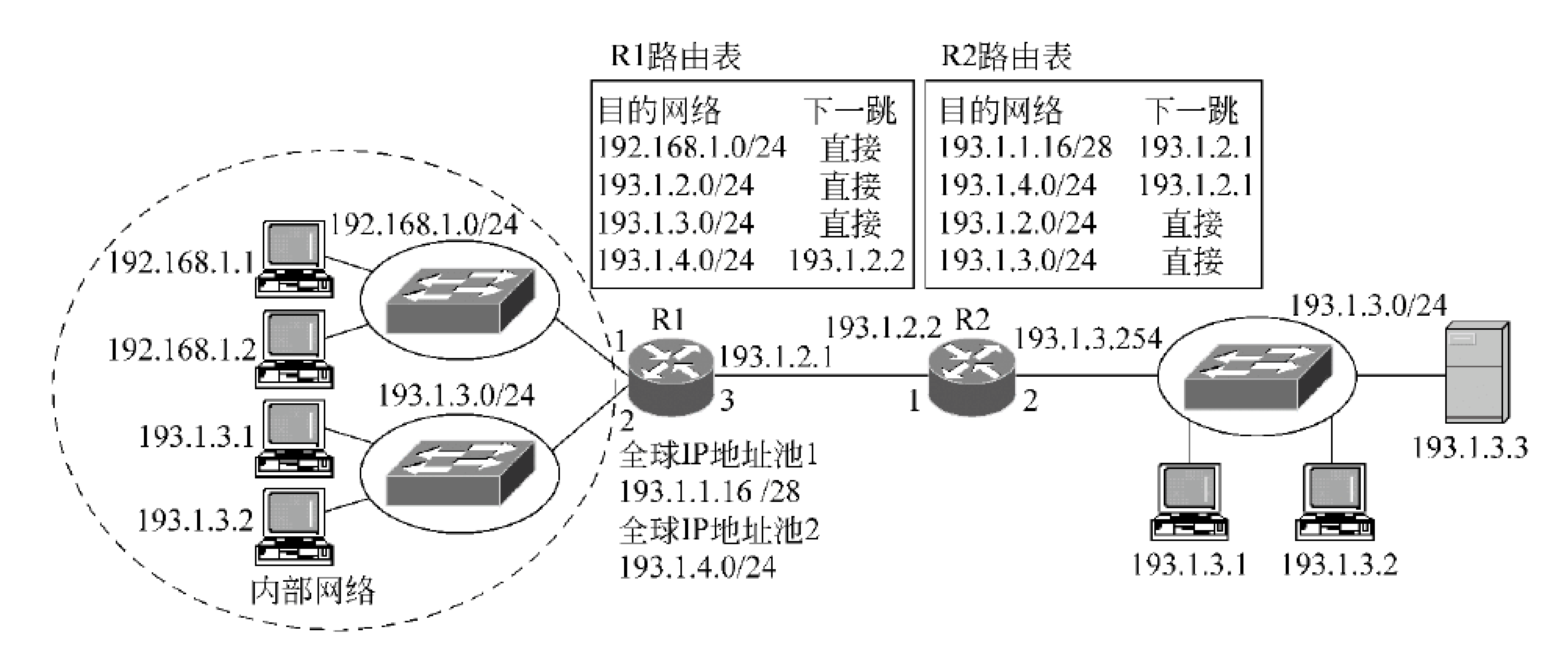


图 2.1 NAT 隐藏内部网络原理图

(2) NAT 允许内部网络分配与外部网络相同的全球 IP 地址。

图 2.1 中,内部网络分配了与外部网络相同的全球 IP 地址 193.1.3.0/24,这种情况下,如果内部网络中的终端需要访问外部网络中的资源,不能以属于网络地址 193.1.3.0/24 的 IP 地址为目的地址,而以路由器 R1 定义的全球 IP 地址池 2(网络地址 193.1.4.0/24)中的某个地址为目的地址,同时路由器 R1 必须建立该全球 IP 地址池 2(193.1.4.0/24)中地址与某个外部网络地址之间的绑定关系。路由器 R1 向外部网络转发内部网络终端发送给外部网络终端的 IP 分组时,需将 IP 分组的目的地址由该全球 IP 地址池 2 中地址转换为与该全球 IP 地址池 2 中地址绑定的外部网络地址。

(3) NAT 表。

NAT 表中的字段如表 2.1 所示。内部本地地址指的是内部网络终端在内部网络中分配的 IP 地址。内部全球地址指的是图 2.1 所示全球 IP 地址池 1 中与该内部网络地址绑定的全球 IP 地址。外部本地地址是内部网络中的终端用于在内部网络中标识外部网络中终端的 IP 地址,如果内部网络分配了与外部网络相同的网络地址,必须用图 2.1 所示的全球 IP 地址池 2 中 IP 地址作为外部本地地址。外部全球地址是外部网络终端分配的全球 IP 地址。如果实现内部网络中本地 IP 地址为 192.168.1.1 的终端与外部网络中 IP 地址为 193.1.3.1 的终端通信,路由器 R1 的 NAT 表如表 2.1 所示,地址转换过程如图 2.2 所示。

表 2.1 NAT 表

内部本地地址	内部全球地址	外部本地地址	外部全球地址
192.168.1.1	193.1.1.17	193.1.4.1	193.1.3.1

如果内部网络分配的本地地址与外部网络分配的全球 IP 地址之间不存在重叠,则外部本地地址和外部全球地址是相同的,内部网络终端直接以外部网络终端分配的全球 IP 地址访问外部网络终端。

NAT 对于阻止外部网络终端向内部网络终端传播蠕虫是有效的,但对于内部网络

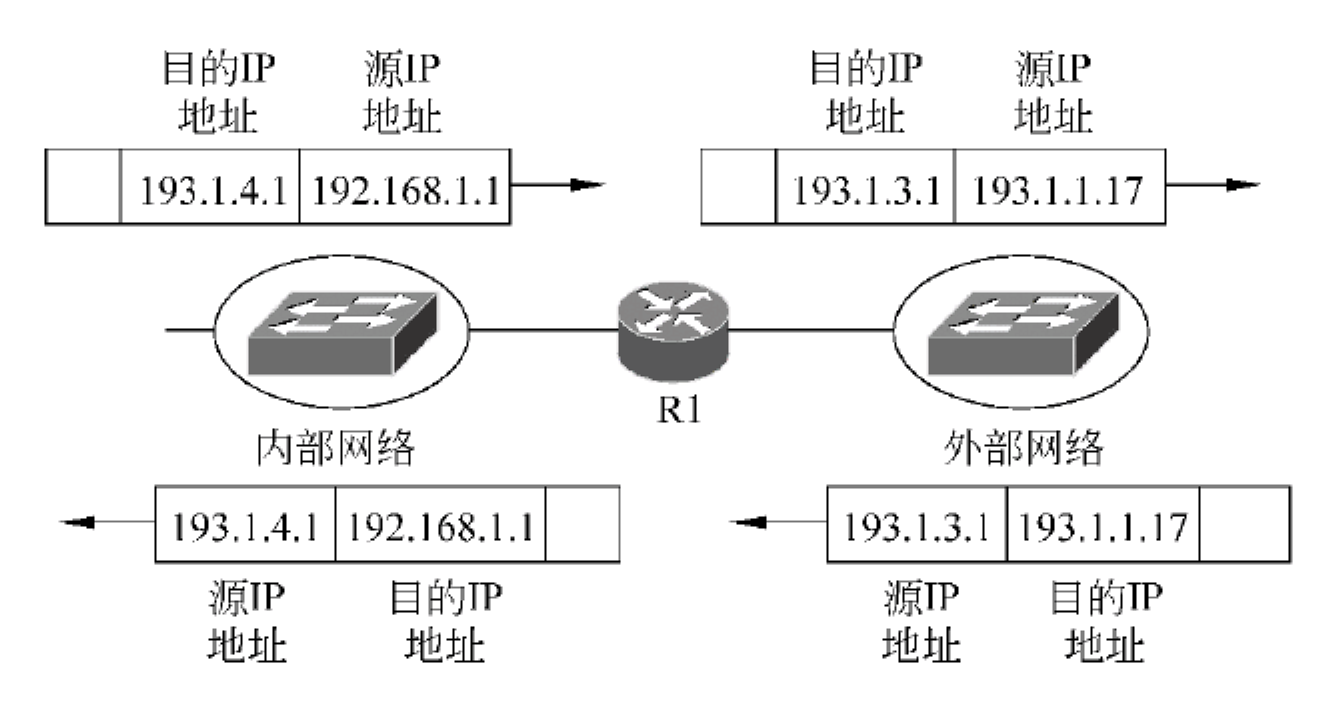


图 2.2　地址转换过程

终端因为打开以感染病毒的宿主程序为附件的邮件，或者通过浏览嵌入病毒的 Web 主页被病毒感染的情况，NAT 是无能为力的，因为无论是接收邮件过程，还是浏览 Web 主页过程，都是由内部网络终端发起的。

2. 防火墙隔断病毒和蠕虫传播途径

1）无状态分组过滤器

（1）过滤规则。

无状态分组过滤器通过规则从 IP 分组流中鉴别出一组 IP 分组，然后对其实施规定的操作。规则由一组属性值组成，如果某个 IP 分组携带的信息和构成规则的一组属性值匹配，意味着该 IP 分组和该规则匹配，对该 IP 分组实施相关操作，相关操作有正常转发和丢弃。

构成规则的属性值通常由下述字段组成：

- 源 IP 地址：用于匹配 IP 分组 IP 首部中的源 IP 地址字段值。
- 目的 IP 地址：用于匹配 IP 分组 IP 首部中的目的 IP 地址字段值。
- 源和目的端口号：用于匹配作为 IP 分组净荷的传输层报文首部中源和目的端口号字段值。
- 协议类型：用于匹配 IP 分组首部中的协议字段值。

一个过滤器可以由多个规则构成，IP 分组只有和当前规则不匹配时才继续和后续规则进行匹配操作，如果和过滤器中的所有规则都不匹配，对 IP 分组进行默认操作。IP 分组一旦和某个规则匹配，则对其实施相关操作，不再和其他规则进行匹配操作。因此，IP 分组和规则的匹配操作顺序直接影响该 IP 分组所匹配的规则，也因此确定了对该 IP 分组实施的操作。

无状态分组过滤器可以作用于接口的输入或输出方向，输入或输出方向针对无状态分组过滤器而言，从外部进入无状态分组过滤器称为输入，离开无状态分组过滤器称为输出。如果作用于输入方向，每一个输入 IP 分组都和过滤器中的规则进行匹配操作；如果和某个规则匹配，则对其实施相关操作；如果实施的操作是丢弃，不再对该 IP 分组进行后续的转发处理。如果过滤器作用于输出方向，则只有当该 IP 分组确定从该接口输出时才将该 IP 分组和过滤器中的规则进行匹配操作。

(2) 过滤规则举例。

网络结构如图2.3所示。分别写出作用于路由器R1接口1输入方向,路由器R2接口2输入方向,实现只允许终端A访问Web服务器,终端B访问FTP服务器,禁止其他一切通信的访问控制的过滤规则。

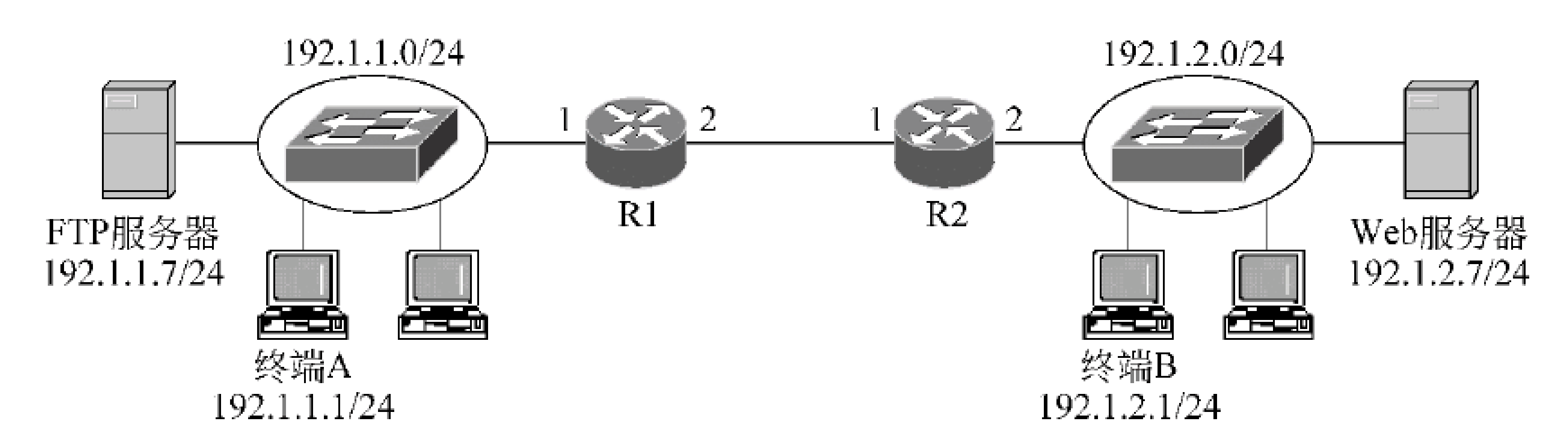


图2.3 网络结构

路由器R1接口1输入方向过滤规则如下:

① 协议=TCP,源IP地址=192.1.1.1/32,源端口号=*,目的IP地址=192.1.2.7/32,目的端口号=80;正常转发。

② 协议=TCP,源IP地址=192.1.1.7/32,源端口号=20,目的IP地址=192.1.2.1/32,目的端口号=*;正常转发。

③ 协议=TCP,源IP地址=192.1.1.7/32,源端口号=21,目的IP地址=192.1.2.1/32,目的端口号=*;正常转发。

④ 协议=IP,源IP地址=*,目的IP地址=*;丢弃。

路由器R2接口2输入方向过滤规则如下:

① 协议=TCP,源IP地址=192.1.2.1/32,源端口号=*,目的IP地址=192.1.1.7/32,目的端口号=20;正常转发。

② 协议=TCP,源IP地址=192.1.2.1/32,源端口号=*,目的IP地址=192.1.1.7/32,目的端口号=21;正常转发。

③ 协议=TCP,源IP地址=192.1.2.7/32,源端口号=80,目的IP地址=192.1.1.1/32,目的端口号=*;正常转发。

④ 协议=IP,源IP地址=*,目的IP地址=*;丢弃。

路由器R1接口1输入方向过滤规则①表明只允许终端A以HTTP访问Web服务器的TCP报文继续正常转发。过滤规则②表明只允许属于FTP服务器和终端B之间控制连接的TCP报文继续正常转发。过滤规则③表明只允许属于FTP服务器和终端B之间数据连接的TCP报文继续正常转发。过滤规则④表明丢弃所有不符合上述过滤规则的IP分组。路由器R2接口2输入方向过滤规则的作用与此相似。

(3) Cisco访问控制列表实现。

路由器R1接口1输入方向配置的Cisco访问控制列表如下:

```
access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq 80
access-list 101 permit tcp host 192.1.1.7 eq 20 host 192.1.2.1
access-list 101 permit tcp host 192.1.1.7 eq 21 host 192.1.2.1
```

```
access-list 101 deny ip any any
```

上述访问控制列表中 101 是编号，属于同一访问控制列表的过滤规则必须具有相同的编号。permit 是实施的操作，允许正常转发。tcp 是协议类型，表示是 TCP 报文。host 192.1.1.1 表示源 IP 地址为 192.1.1.1/32，如果源 IP 地址为网络地址 192.1.1.0/24，需用 192.1.1.0 0.0.0.255 表示，其中 192.1.1.0 是网络地址，0.0.0.255 是子网掩码 255.255.255.0 的反码。host 192.1.2.7 表示目的 IP 地址为 192.1.2.7/32。紧随源 IP 地址的是源端口号，紧随目的 IP 地址的是目的端口号，所以在上述访问控制列表中，eq 80 表示目的端口号等于 80，eq 20 表示源端口号等于 20。deny 是拒绝操作，丢弃该 IP 分组。any 表示任意 IP 地址，也可用 0.0.0.0 255.255.255.255 表示，这里 0.0.0.0 表示任意网络，255.255.255.255 表示网络前缀位数是 0。以此得出，host 192.1.1.1 可以表示为 192.1.1.1 0.0.0.0，0.0.0.0 表示网络前缀位数是 32。

Cisco 访问控制列表的默认过滤规则是过滤规则④，因此配置 Cisco 访问控制列表时，无需配置过滤规则④。

路由器 R2 接口 2 输入方向配置的 Cisco 访问控制列表如下：

```
access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 eq 20
access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 eq 21
access-list 102 permit tcp host 192.1.2.7 eq 80 host 192.1.1.1
access-list 102 deny ip any any
```

2）有状态分组过滤器

（1）有状态分组过滤器实现原理。

如果要求实现只允许图 2.3 中终端 A 发起访问 Web 服务器，不允许网络存在其他通信过程的访问控制，路由器 R1 接口 1 输入方向和路由器 R2 接口 2 输入方向设置如下过滤规则：

路由器 R1 接口 1 输入方向过滤规则如下：

① 协议＝TCP，源 IP 地址＝192.1.1.1/32，源端口号＝*，目的 IP 地址＝192.1.2.7/32，目的端口号＝80；正常转发。

② 协议＝IP，源 IP 地址＝*，目的 IP 地址＝*；丢弃。

路由器 R2 接口 2 输入方向过滤规则如下：

① 协议＝TCP，源 IP 地址＝192.1.2.7/32，源端口号＝80，目的 IP 地址＝192.1.1.1/32，目的端口号＝*；正常转发。

② 协议＝IP，源 IP 地址＝*，目的 IP 地址＝*；丢弃。

需要强调的是，真正实现只允许终端 A 发起访问 Web 服务器，不允许网络存在其他通信过程的访问控制需要做到：

① 只允许由终端 A 发起建立与 Web 服务器之间的 TCP 连接。

② 只允许属于由终端 A 发起建立的与 Web 服务器之间的 TCP 连接的 TCP 报文沿着 Web 服务器至终端 A 方向传输。

③ 必须由终端 A 发出访问 Web 服务器资源的请求消息，然后由 Web 服务器返回对

应的响应消息。

但上述过滤规则中直接允许 Web 服务器发送的、源端口号为 80 的 TCP 报文沿着 Web 服务器至终端 A 方向传输,一是没有规定这种传输过程必须在由终端 A 发起建立与 Web 服务器之间的 TCP 连接后进行;二是由于需要用两端插口标识 TCP 连接,因此上述过滤规则并没有明确指出只有属于由终端 A 发起建立与 Web 服务器之间的 TCP 连接的 TCP 报文才能沿着 Web 服务器至终端 A 方向传输;三是没有检测 Web 服务器传输给终端 A 的 TCP 报文是否是终端 A 发送的请求消息对应的响应消息。

真正实现只允许终端 A 发起访问 Web 服务器,不允许网络存在其他通信过程的访问控制的思路应该这样:

① 终端 A 至 Web 服务器传输方向上的过滤规则允许传输与完成由终端 A 发起访问 Web 服务器的操作有关的 TCP 报文。

② 初始状态下,Web 服务器至终端 A 传输方向上的过滤规则拒绝一切 IP 分组传输。

③ 只有当终端 A 至 Web 服务器传输方向上传输了与终端 A 发起访问 Web 服务器的操作有关的 TCP 报文后,Web 服务器至终端 A 传输方向才允许传输作为对应响应消息的 TCP 报文。

(2) Cisco 有状态分组过滤器实现机制。

针对图 2.3 所示的网络结构,Cisco 通过访问控制列表允许与终端 A 访问 Web 服务器有关的 TCP 报文沿着终端 A 至 Web 服务器方向传输,但通过访问控制列表阻止一切 TCP 报文沿着 Web 服务器至终端 A 方向传输。但在终端 A 至 Web 服务器方向启动检测(Inspect)机制,一旦检测到与终端 A 访问 Web 服务器有关的 TCP 报文,在反方向(Web 服务器至终端 A 方向)动态增加允许该 TCP 报文对应的响应报文传输的过滤规则。这样,通过访问控制列表允许与终端 A 访问 Web 服务器有关的 TCP 报文沿着终端 A 至 Web 服务器方向传输,通过检测机制允许作为该 TCP 报文的响应报文沿着 Web 服务器至终端 A 方向传输,允许沿着 Web 服务器至终端 A 方向传输的 TCP 报文必须是访问控制列表允许沿着终端 A 至 Web 服务器方向传输的 TCP 报文的响应报文。

路由器 R1 接口 1 输入方向和路由器 R2 接口 2 输出方向(终端 A 至 Web 服务器传输方向)设置如下访问控制列表:

```
access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www
```

该访问控制列表允许源 IP 地址=192.1.1.1/32、目的 IP 地址=192.1.2.7/32、源端口号任意、目的端口号=HTTP 对应的著名端口号(80)的 TCP 报文正常转发。

路由器 R1 接口 1 输出方向和路由器 R2 接口 2 输入方向(Web 服务器至终端 A 传输方向)设置如下访问控制列表:

```
access-list 102 deny ip any any
```

该访问控制列表禁止一切 IP 分组继续传输。

但需要创建如下检测机制:

```
ip inspect name a101 http
```

a101 是检测机制名，http 是需要检测的应用层协议。该检测机制表示如果在指定方向检测到属于 http 且该方向访问控制列表允许正常转发的 TCP 报文，在相反方向动态增加允许该 TCP 报文对应的响应报文正常转发的过滤规则。

该检测机制必须作用在路由器 R1 接口 1 输入方向和路由器 R2 接口 2 输出方向。

Cisco 将有状态分组过滤器实现机制称为基于上下文的访问控制(Context-Based Access Control，CBAC)机制。

3. 网络入侵防御系统隔断病毒和蠕虫传播途径

网络入侵防御系统的功能是捕获信息流，然后对捕获到的信息流进行检测，一旦检测到异常信息流，执行反制动作。对于图 2.4 所示网络结构，网络入侵防御系统工作在转发模式，必须经它转发流经它所在链路的信息流，因此不存在捕获信息流的问题。检测信息流异常的前提是用于实施病毒和蠕虫传播的信息流与完成正常访问过程的信息流之间存在差异，检测机制就是区分出完成正常访问过程的信息流和实施病毒和蠕虫传播的信息流的机制。

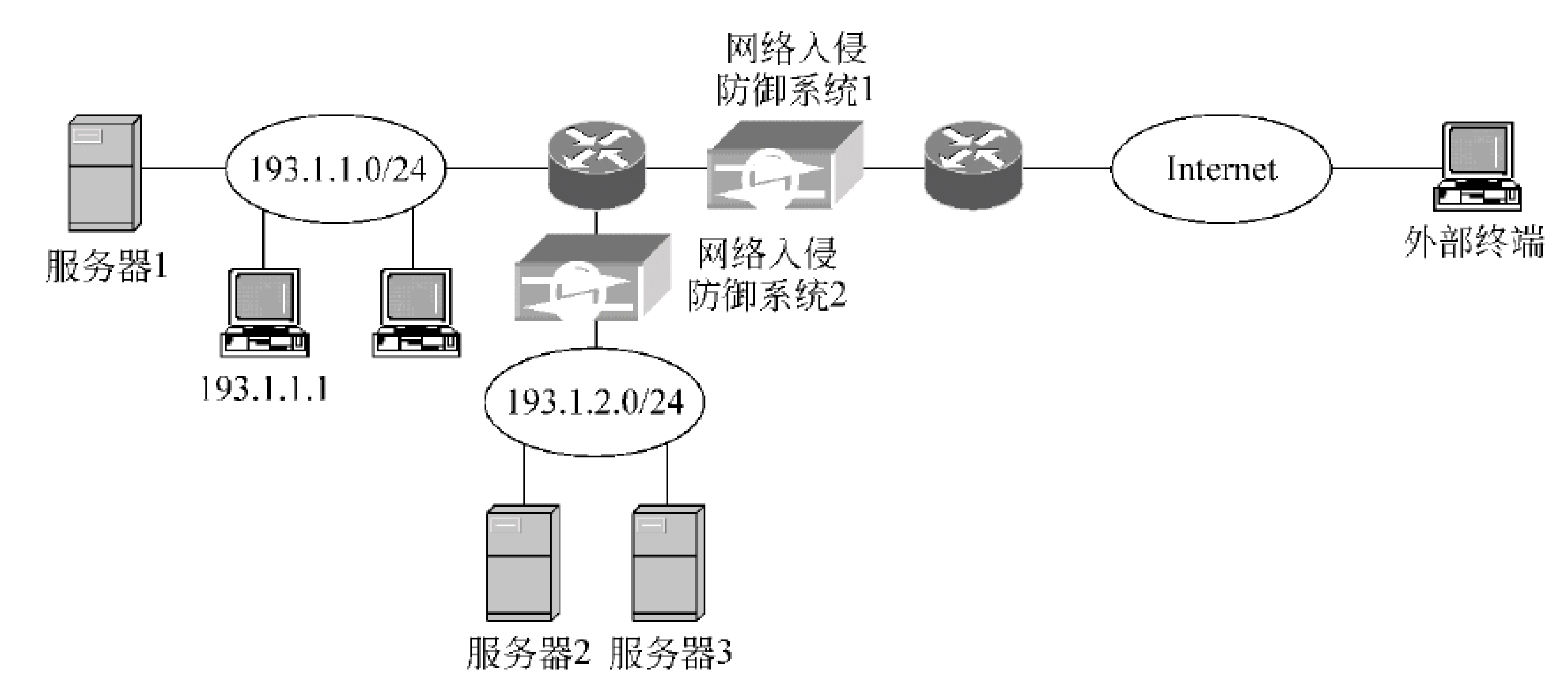


图 2.4　入侵防御系统隔断病毒和蠕虫传播途径原理图

(1) 匹配攻击特征。蠕虫传播通常经过漏洞扫描、渗入攻击对象和入侵攻击对象这样的过程，可以通过分析典型的蠕虫传播过程，提取出完成蠕虫传播过程需要交换的信息流中不同于完成正常访问过程的信息流的一些特征，如果捕获到的信息流中包含某个蠕虫的特征，确定该信息流是用于实施该蠕虫传播的信息流，网络入侵防御系统将阻断该信息流的正常传输。

(2) 设置阈值和制订规则。通过长时间采样、分析完成正常访问过程的信息流和实施病毒和蠕虫传播的信息流，可以得出用于区分它们的一些统计值，如单位时间内某个终端发起建立的 TCP 连接的数量。阈值就是区分完成正常访问过程的信息流和实施病毒和蠕虫传播的信息流的临界值，一旦某个时间段内根据捕获的信息流计算所得的多个统计值超过了对应的阈值，可以判断该信息流是用于实施病毒和蠕虫传播的信息流。规则是长时间采样、分析完成正常访问过程的信息流后得出的行为特征，如终端 C 的行为特征是：8:00～17:00 访问网络资源的概率大于 90%；平均流量是 3Mbps，峰值流量是

30Mbps;流量大于20Mbps的持续时间小于20ms的概率大于98%;发送邮件产生的流量只占总流量的3%等。一旦根据一段时间内捕获的信息流分析出的行为特征偏离规则较多,可以确定是用于实施病毒和蠕虫传播的信息流,如根据一段时间内捕获的信息流分析出的终端C的行为特征:16:00~22:00持续发送信息流,平均流量为35Mbps,流量大于40Mbps的持续时间大于50ms的概率达到70%,发送邮件产生的流量占总流量的40%,可以断定是终端C因为病毒或蠕虫发作,向外大量发送以感染病毒的宿主程序为附件的邮件,以此向其他终端传播病毒。

(3)设置访问控制策略。通过设置访问控制策略,只允许符合访问控制策略的信息交换过程进行。

网络入侵防御系统与NAT和防火墙不同的地方是网络入侵防御系统不仅能够控制内网与外网之间交换的信息流,如图2.4中网络入侵防御系统1,而且还能控制内网中不同网段之间交换的信息流,如图2.4中网络入侵防御系统2。通过合理放置网络入侵防御系统,可以检测流经任何链路的信息流,并对异常信息流进行反制。

4. 流量管制抑制病毒和蠕虫传播

某个终端如果正在传播病毒,某种类型的信息流的流量就会剧增。如果某个终端通过向外大量发送以感染病毒的宿主程序为附件的邮件实现向其他终端传播病毒的目的,该终端与发送邮件相关的信息流的流量就会剧增。同样,如果某个终端正在传播蠕虫,与漏洞扫描有关的信息流的流量就会剧增,如源地址相同、目的地址不同的ICMP ECHO请求报文,源和目的地址相同、目的端口不同的建立TCP连接请求报文。如果网络能够对每一个终端与传播典型病毒和蠕虫有关的信息流的流量实施管制,将其限制在完成正常访问过程需要的流量范围内,就可有效抑制病毒和蠕虫传播。图2.5中,如果对进出路由器接口1和2与传播典型病毒和蠕虫有关的信息流的流量实施管制,将有效抑制病毒和蠕虫在内部网络不同网段之间的传播。

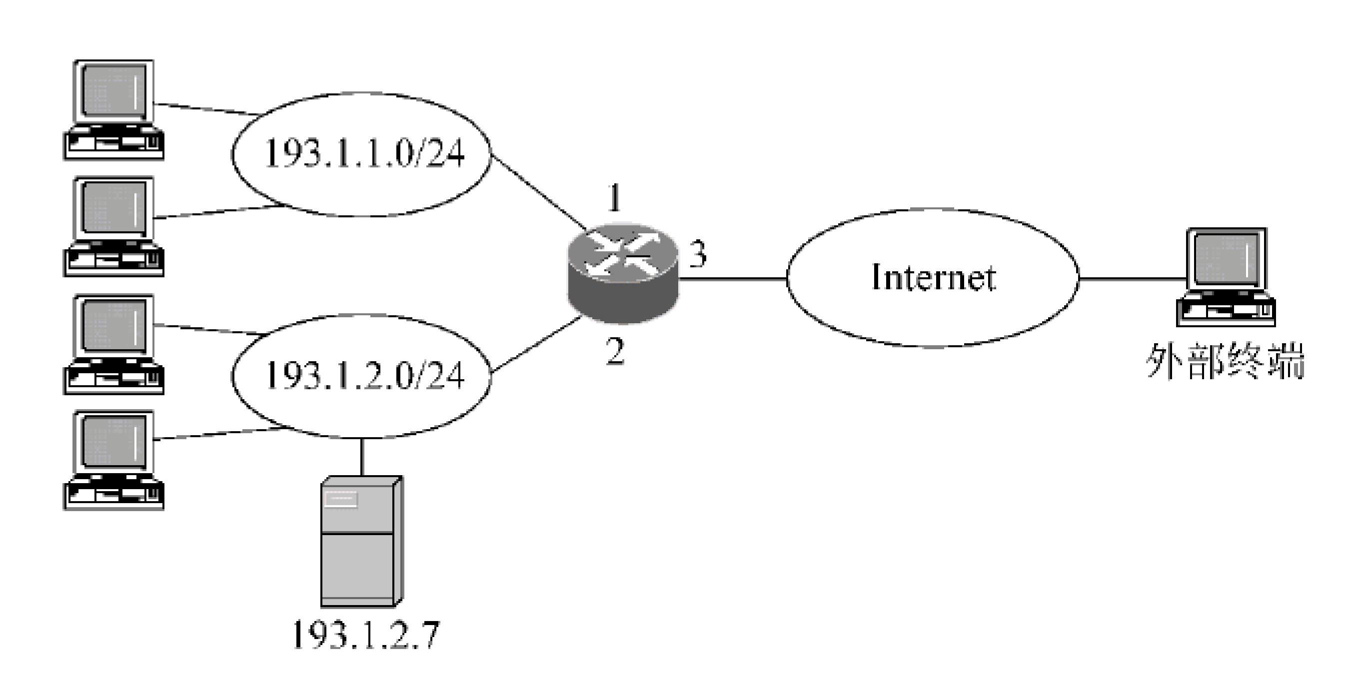


图2.5 流量管制限制病毒和蠕虫传播原理图

2.1.4 网络安全技术对减少恶意代码危害的作用

破坏主机系统一般由主机系统自身安全技术解决,如主机入侵防御系统、查杀病毒软件和系统备份等。网络安全技术阻止病毒和蠕虫传播的原理和过程已在2.1.3节进行讨论,这里重点讨论网络安全技术阻止非法访问和拒绝服务攻击的原理和过程。

1. 网络安全技术阻止非法访问

非法访问主要发生在外网终端对内部中的信息资源的访问过程,因此防火墙是阻止非法访问发生的有效工具。

(1) 访问控制策略禁止远程登录内部网络终端。

病毒的一大危害是建立拥有管理员权限的账户,并打开 Telnet 服务,或者运行远程桌面控制系统的服务器端程序,使得外部网络终端可以远程登录主机系统,访问主机系统资源。通过配置防火墙的访问控制策略禁止外部网络终端通过 Telnet 或远程桌面控制系统的客户端程序远程登录内部网络中的主机系统。

(2) 访问控制策略禁止木马向外发送信息资源。

木马采用客户端/服务器结构,由客户端和服务器端代码组成,激活服务器端代码后,黑客通过启动客户端代码和服务器端建立连接,并通过客户端对服务器端系统进行操作,其过程类似于用 Telnet 实现远程登录。由于木马主要用于窃取内部网络资源,而内部网络往往使用本地 IP 地址,由互连内部网络和外部网络的边界路由器实现网络地址转换功能。因此,当黑客终端连接在外部网络时,无法由外部网络终端发起与内部网络终端之间的 TCP 连接。这种情况下,首先需要启动客户端代码,由客户端代码负责侦听某个端口,一旦激活服务器端代码,由服务器端代码发起与客户端之间的 TCP 连接,并在成功建立连接后,在客户端生成一个表示特定服务器端的图标,黑客双击该图标,弹出服务器端的资源管理界面,黑客可以对服务器端的资源进行操作。

通过配置防火墙的访问控制策略对内部网络终端发起建立的与外部网络终端之间的 TCP 连接,及经过 TCP 连接传输的 TCP 报文进行严格监控,使得木马服务器端与外部网络中的木马客户端之间很难建立符合访问控制策略的 TCP 连接,即使它们之间成功建立 TCP 连接,也很难通过符合访问控制策略的 TCP 报文交换过程完成木马客户端对木马服务器端所在主机系统的非法访问过程。

2. 网络安全技术阻止拒绝服务攻击

(1) 防火墙阻止外部网络终端对内部网络终端实施 SYN 泛洪攻击。

为了阻止外部网络终端对内部网络终端实施 SYN 泛洪攻击,在防火墙连接外部网络接口启动防 SYN 泛洪攻击机制,它的操作过程如下:首先设定开始释放操作的未完成 TCP 连接数和终止释放操作的未完成 TCP 连接数,防火墙同步记录下由经过防火墙转发的建立 TCP 连接请求报文导致的未完成的 TCP 连接,一旦未完成的 TCP 连接数达到设定的开始释放操作的未完成 TCP 连接数,防火墙按照这些未完成的 TCP 连接的建立顺序释放一部分未完成的 TCP 连接,释放操作是向未完成的 TCP 连接的两端发送 RST=1的复位控制报文。这个释放过程一直进行,直到未完成的 TCP 连接数等于设定的终止释放操作的未完成 TCP 连接数为止。

(2) 网络入侵防御系统检测与反制拒绝服务攻击。

分布式网络入侵防御系统如图 2.6 所示。由多个探测器和一台管理服务器组成,每一个探测器负责检测流经某个网段的信息流,并将检测结果报告给管理服务器,管理服务器通过综合这些探测器的检测结果确定是否发生 DDoS(Distributed Denial of Service,分布式拒绝服务)攻击,并通过向探测器发送命令要求探测器丢弃属于 DDoS 攻击的分组。

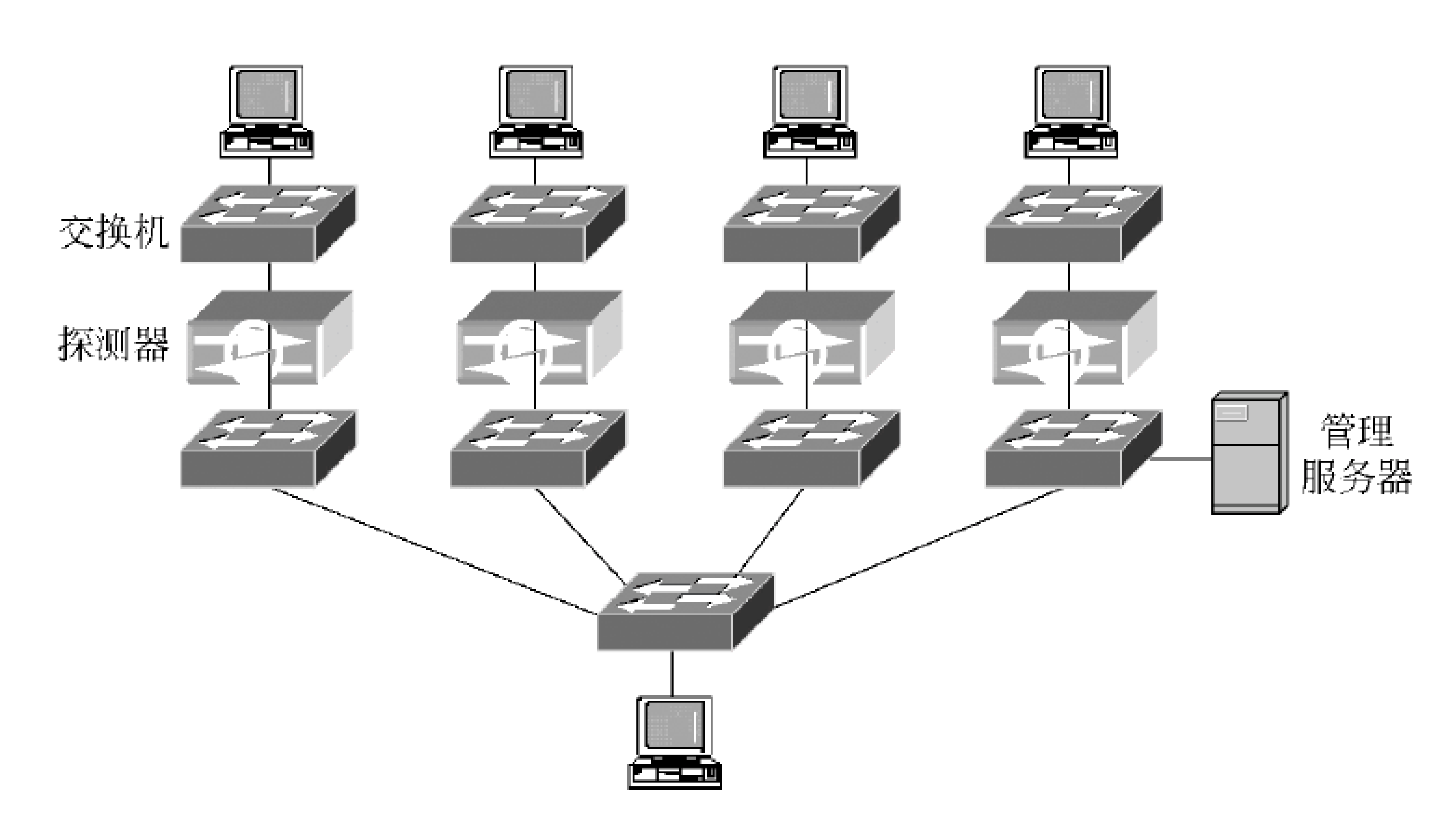


图 2.6 分布式网络入侵防御系统

(3) 流量管制抑制拒绝服务攻击。

可以通过在图 2.5 所示网络中路由器接口 1 和 3 的输入方向、接口 2 输出方向限制目的地址为 193.1.2.7 的 ICMP ECHO 响应报文或是 UDP 报文的流量，抑制由内部网络终端和外部网络终端发起的对图 2.5 中 IP 地址为 193.1.2.7 的服务器的拒绝服务攻击。

2.2 例题解析

2.2.1 自测题

1. 选择题

(1) 下述________表示黑客们编写的旨在破坏其他主机系统的代码集合。

A. 恶意代码 B. 病毒 C. 木马 D. 蠕虫

(2) 下述________表示黑客们编写的旨在非法访问其他主机系统中信息资源的代码。

A. 恶意代码 B. 病毒 C. 木马 D. 蠕虫

(3) 下述________表示黑客们编写的、嵌入在正常程序中，具有自我复制能力的一段代码。

A. 恶意代码 B. 病毒 C. 木马 D. 蠕虫

(4) 下述________表示黑客们编写的、具有自动传播和自动激活特性的完整程序。

A. 恶意代码 B. 病毒 C. 木马 D. 蠕虫

(5) 蠕虫能够自动传播到某个主机系统并自动激活的原因是________。

A. 主机系统存在漏洞

B. 主机系统下载程序

C. 主机系统收发邮件

D. 主机系统之间用移动媒介复制文件

(6) 下述________操作与传播病毒无关。

A. 运行补丁软件

B. 主机系统下载程序

C. 主机系统收发邮件

D. 主机系统之间用移动媒介复制文件

(7) 下述________操作不属于病毒感染。

A. 病毒将自身插入引导程序　　B. 病毒将自身插入可执行文件

C. 宏病毒将自身插入 Office 文档　　D. 建立具有管理员权限的账户

(8) 下述________不是阻止病毒传播的措施。

A. 运行补丁软件　　B. 安装查杀病毒软件

C. 禁止读写移动存储媒介　　D. 对主机系统中的重要文件加密

(9) 下述________不是阻止病毒经过网络传播的措施。

A. 运行补丁软件　　B. 安装查杀病毒软件

C. 禁止读写移动存储媒介　　D. 安装主机入侵防御系统

(10) 下述________不是阻止病毒实施破坏操作的措施。

A. 安装主机入侵防御系统

B. 监控内部网络终端发起建立的 TCP 连接

C. 禁止读写移动存储媒介

D. 对主机系统中的重要文件加密

(11) 下述________不是恶意代码的危害。

A. 删除文件　　B. 向其他主机系统传播病毒

C. 非法访问主机系统资源　　D. 断开主机系统和网络的连接

(12) 下述________病毒的变种处理对避免病毒被基于特征的扫描技术发现是无效的。

A. 压缩病毒　　B. 用随机产生的密钥加密病毒

C. 随机插入无效代码　　D. 指令同义替换

(13) 下述________病毒检测机制是检测系统软件是否感染病毒的有效方法。

A. 基于特征的扫描技术　　B. 基于线索的扫描技术

C. 基于完整性检测的扫描技术　　D. 基于行为的检测技术

(14) 下述________不是网络成为病毒快速传播通道的原因。

A. 利用主机系统漏洞自动传播病毒

B. 通过邮件传播病毒

C. 通过 Web 页面传播病毒

D. 通过移动存储媒介在主机系统间相互复制文件传播病毒

(15) 防火墙能有效阻止下述________病毒传播方式。

A. 利用主机系统漏洞自动传播病毒　　B. 通过邮件传播病毒

C. 通过 Web 页面传播病毒　　D. 通过实用程序传播病毒

(16) 网络入侵防御系统对下述________病毒传播方式不起作用。

A. 利用主机系统漏洞自动传播病毒　　B. 通过邮件传播病毒
C. 通过 Web 页面传播病毒　　D. 通过实用程序传播病毒

2. 填空题

(1) 目前常见的恶意代码包括________、________、________和________。

(2) 目前常见的基于主机系统的防病毒措施包括________、________和________，其中________的作用是发现正在运行的病毒和被病毒感染的文件，________的作用是关闭病毒传播到主机系统的通路，________的作用是监控病毒感染主机系统过程。

(3) 目前常见的基于网络的防病毒措施包括________、________、________和________，其中________的作用是隐藏内部网络，使外部网络终端无法发现内部网络中的终端，________的作用是通过控制内部网络和外部网络之间的信息交换过程隔断病毒向内部网络传播的通路，________的作用是通过监控流经关键链路的信息流发现病毒并隔断病毒传播通路，________的作用是通过管制疑似与病毒传播有关的信息流的流量来抑制病毒传播。

(4) 狭义病毒的主要特征是________和________，蠕虫的主要特征是________、________和________，木马的主要特征是________，木马的特征是功能特征，与________和________无关，因此可以有狭义病毒的木马和蠕虫木马。

(5) 病毒发作时实施的破坏动作主要包括________、________、________和________，其中主机入侵防御系统对阻止________和________有用，防火墙和网络入侵防御系统对阻止________、________和________有用，NAT 对阻止________和________有用，流量管制对阻止________和________有用。

(6) 病毒的 4 个阶段是________、________、________和________。

3. 名词解释

____逻辑炸弹　　____查杀病毒软件
____恶意代码　　____狭义病毒
____蠕虫　　____木马
____感染病毒　　____病毒发作
____变形病毒　　____恶意移动代码
____宏病毒　　____病毒传播

(a) 黑客们编写的旨在破坏其他主机系统的代码集合。

(b) 一段需要寄生在别的程序中的代码，激发后，可以将自己反复插入到其他程序中，并在条件成熟时实施破坏动作。

(c) 一种具备完整程序特性的恶意代码，能够自动传播到其他系统，并具有自动激发功能，因而能够快速传播。

(d) 一种恶意代码，其主要功能在于削弱主机系统的安全性，并盗取主机系统的信息资源。

(e) 一段通常通过人工嵌入在正常程序中的恶意代码，一旦出现激发该恶意代码的条件，恶意代码将对主机系统实施破坏。

(f) 一种能够对进程的执行过程实施动态监测，以发现激活的病毒，并能够对主机系

统中的文件和可能隐藏病毒处(如引导扇区)实施扫描,以发现感染病毒的文件和隐藏的病毒的软件。

(g) 一种每一次感染过程都改变一下自身形态,甚至发作时的行为的病毒。

(h) 一种具有恶意代码特性的、浏览网页时需要从服务器下载到本地执行的小型程序。

(i) 一种嵌入在 Office 文档中、具有病毒特征的宏,宏是一段打开文档时由应用程序执行的代码。

(j) 一台感染病毒的主机系统使另一台主机系统感染相同病毒的过程。

(k) 使主机系统中存在感染病毒的可执行文件,且通过修改主机系统配置保证病毒能够被再次激活的过程。

(l) 病毒激活时,因为满足特定条件而使病毒除了进行感染其他文件的操作外,还进行其他对主机系统和网络具有危害的操作的现象。

4. 判断题

(1) 只要安装杀毒软件,定时更新病毒特征库,就不可能感染病毒。

(2) 操作系统和应用程序漏洞是蠕虫入侵的主要渠道。

(3) 木马不可能具备狭义病毒特征。

(4) 木马不可能具备蠕虫特征。

(5) 网络是病毒快速传播通道。

(6) 病毒发作意味着破坏主机系统,使其不能正常运行。

(7) 主机系统安装查杀病毒软件、个人防火墙和主机入侵防御系统是防止病毒侵入的有效措施。

(8) 网络安全技术能够解决病毒传播问题。

(9) 防火墙能够配置杜绝病毒传播到内部网络的访问控制策略。

(10) 网络入侵防御系统能够检测出一切流经它所在链路的病毒并予以丢弃。

2.2.2 自测题答案

1. 选择题答案

(1) A,恶意代码就是所有用于破坏其他主机系统的代码的统称。

(2) C,木马的主要功能就是非法访问其驻留主机系统的信息资源。

(3) B,狭义病毒的特征:一是需要宿主程序,二是具有自我复制能力。

(4) D,蠕虫的特征:一是完整程序,二是能够在不需要人力介入的情况下自动传播和自动激活。

(5) A,蠕虫通过利用主机系统漏洞实现自动传播和自动激活。

(6) A,运行补丁软件可以阻止病毒传播,其他三项操作可以传播病毒。

(7) D,这一项不属于感染病毒,而是病毒发作时实施的破坏操作。

(8) D,这一项与阻止病毒传播无益,但可以减轻病毒发作时对主机系统中信息资源的保密性的破坏。

(9) C,经过网络传播病毒时不需要读写移动存储媒介。

(10) C,其他三项可以阻止病毒破坏主机系统、向其他主机系统非法传输信息、保证主机系统信息资源的保密性。

(11) D,病毒造成的危害大多需要通过网络才能完成,断开网络应该是减少危害扩散的措施。

(12) A,每一次变形处理后的结果都应不同,同一段代码每一次压缩处理的结果是相同的。

(13) C,对较长时间内不变的系统软件适合采用基于完整性检测的扫描技术,用该扫描技术可以发现任何被病毒感染的文件。

(14) D,该病毒传播方式与网络无关。

(15) A,防火墙只能通过访问控制策略禁止一些信息交换过程,其他三种传播方式往往利用访问控制策略允许进行的信息交换过程进行病毒传播。

(16) D,通过攻击特征匹配和访问控制策略能发现 A 传播方式。通过精心设置阈值和规则也能发现 B 传播方式。通过深入检查、分析一段时间内相互交换的信息可以发现 C 传播方式。除非实用程序包含已经提取出病毒特征的病毒,且网络入侵防御系统具有根据病毒特征库查杀病毒的功能,否则静态分析某个实用程序是否包含病毒是很难的。

2. 填空题答案

(1) 狭义病毒,蠕虫,木马,逻辑炸弹。

(2) 查杀病毒软件,个人防火墙,主机入侵防御系统,查杀病毒软件,个人防火墙,主机入侵防御系统。

(3) NAT,防火墙,网络入侵防御系统,流量管制,NAT,防火墙,网络入侵防御系统,流量管制。

(4) 嵌入宿主程序的一段代码,具有自我复制能力,完整程序,自动传播,自动激活,提供实现远程非法访问的通路,代码形式,传播方式。

(5) 破坏主机系统,实现非法访问,传播病毒,实施拒绝服务攻击,破坏主机系统,实现非法访问,传播病毒,实现非法访问,实施拒绝服务攻击,实现非法访问,传播病毒,传播病毒,实施拒绝服务攻击。

(6) 静寂阶段,传播阶段,触发阶段,执行阶段。

3. 名词解释答案

e 逻辑炸弹	f 查杀病毒软件
a 恶意代码	b 狭义病毒
c 蠕虫	d 木马
k 感染病毒	l 病毒发作
g 变形病毒	h 恶意移动代码
i 宏病毒	j 病毒传播

4. 判断题答案

(1) 错,目前大多数杀毒软件都是基于病毒特征的,通常都是在发现病毒造成的后果后,才会发现病毒,分析病毒,提取病毒特征。

(2) 对，蠕虫通常通过目标主机操作系统和应用程序的漏洞上传到目标主机，并自动激活。

(3) 错，木马是根据其功能特征分类的结果，狭义病毒是根据代码形式和传播方式分类的结果，允许存在具有两者特征的恶意代码。

(4) 错，木马是根据其功能特征分类的结果，蠕虫是根据代码形式与传播和激活方式分类的结果，允许存在具有两者特征的恶意代码。

(5) 对，大量病毒传播方式是依赖网络的。

(6) 错，病毒发作时实施的破坏动作除了破坏主机系统外，还包括传播病毒、实施非法访问、实施拒绝服务攻击等。

(7) 对，这三项是目前主机系统经常采取的防病毒措施。

(8) 错，主机系统安全技术和网络安全技术有机结合也不能完全阻止病毒传播，单靠网络安全技术更是无法解决病毒传播问题。

(9) 错，大量病毒传播过程是通过访问控制策略允许的信息交换过程完成的，除非禁止内部网络和外部网络之间交换信息。

(10) 错，没有一种检测机制能够检测出所有病毒。

2.2.3　简答题解析

1. 简述网络是病毒和蠕虫快速传播通道的理由。

回答：目前常见的病毒和蠕虫传播方式有通过移动存储媒介在主机系统之间相互复制文件、浏览封装恶意移动代码的 Web 主页、打开作为邮件附件的感染病毒的宿主程序、下载并运行感染病毒的实用程序、在共享目录中保存感染病毒的宿主程序、利用主机系统漏洞上传蠕虫或感染病毒的宿主程序。除了通过移动存储媒介传播病毒外，其他传播方式都需通过网络进行，因此网络是病毒和蠕虫快速传播的主要通道。

2. 简述阻止病毒传播和危害发生的措施。

回答：这些措施分为基于主机系统的措施和基于网络的措施。基于主机系统的措施有及时运行补丁软件，安装查杀病毒软件、主机入侵防御系统和个人防火墙等。基于网络的措施有在网络边界设置控制网络间信息交换过程的防火墙，在关键链路设置严格监控流经该段链路的信息流的网络入侵防御系统，采用隐藏内部网络的 NAT 技术和限制疑似与病毒传播和拒绝服务攻击有关的信息流的流量的流量管制技术。

3. 简述恶意代码长期存在的理由。

回答：导致恶意代码存在的主要原因是主机系统的漏洞，包括操作系统漏洞和应用程序漏洞，在未来较长一段时间内，不可能编写出没有安全漏洞的操作系统和应用程序，因此肯定会产生针对各种漏洞的恶意代码。网络是传播恶意代码的主要通道，网络安全技术无法完全阻隔病毒传播通路，也无法完全阻止黑客通过网络扫描到存在漏洞的主机系统，并通过网络将针对该漏洞的恶意代码上传到该主机系统并激活。

2.2.4　综合题解析

网络结构如图 2.7 所示，要求实现：

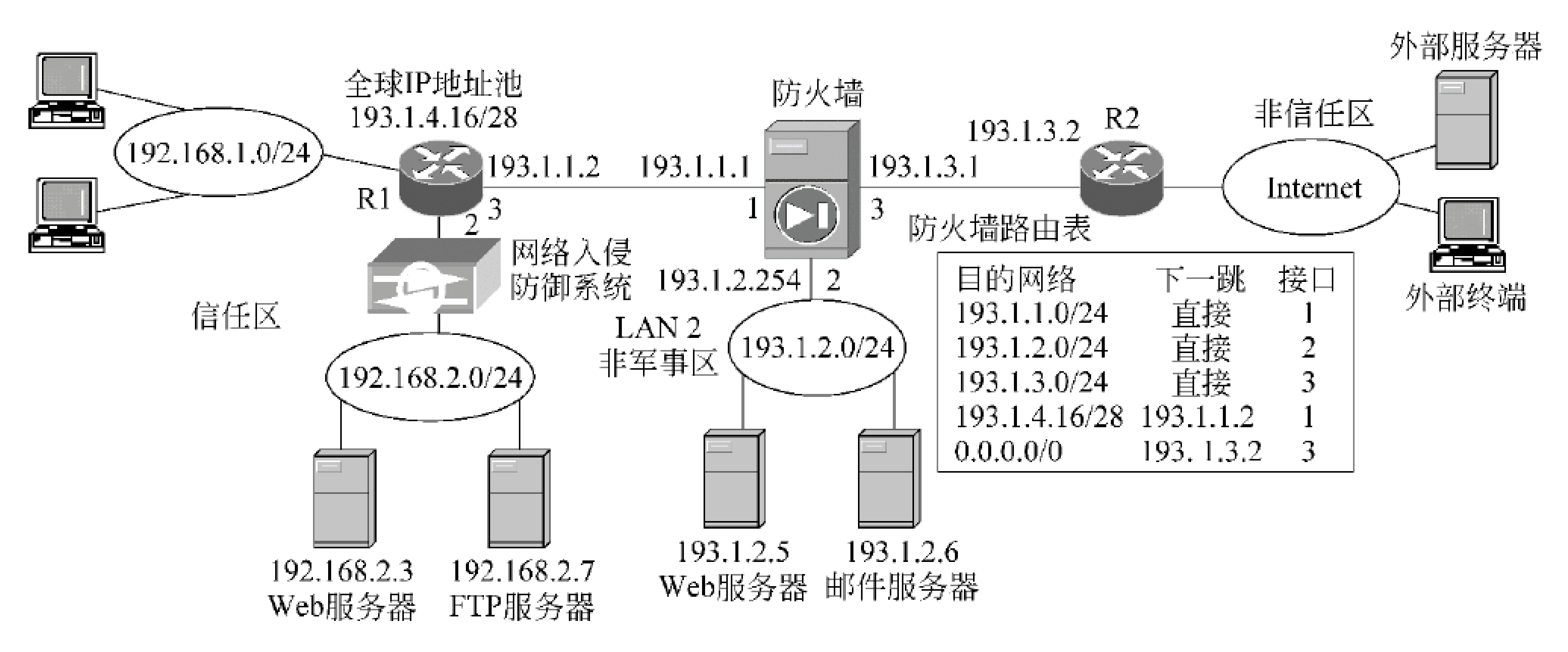


图 2.7 网络结构

(1) 通过 NAT 技术隐藏分配本地 IP 地址的内部网络,外部网络终端无法直接访问内部网络。

(2) 防火墙配置的访问控制策略能够实现:允许内部网络终端访问非军事区中的 Web 服务器和邮件服务器;允许内部网络终端访问非信任区中的 Web 服务器;允许非军事区中的邮件服务器与非信任区中的邮件服务器相互交换邮件;允许非信任区中的终端访问非军事区中的 Web 服务器。

(3) 路由器 R1 配置的分组过滤器能够实现:进入网络 192.168.2.0/24 的只能是与内部网络终端访问 Web 服务器和 FTP 服务器相关的 TCP 报文。

(4) 网络入侵防御系统配置的访问控制策略能够实现:经过网络入侵防御系统转发的只能是与内部网络终端访问 Web 服务器和 FTP 服务器相关的 TCP 报文;通过加载攻击特征库能够检测出与内部网络终端利用 Web 服务器和 FTP 服务器漏洞实施入侵相关的信息流并予以反制;通过设置阈值和规则能够检测出与内部网络终端进行的扫描和对 Web 服务器、FTP 服务器实施的拒绝服务攻击有关的信息流并予以反制。

(5) 通过在路由器 R1 接口 1 配置流量管制器限制经过路由器 R1 接口 1 输出的与发送邮件和传输 ICMP ECHO 请求和响应报文有关的信息流的流量。

解析:(1) 路由器 R1 配置 NAT 功能,接口 1 为连接内部网络接口,接口 3 为连接外部网络接口,配置全球 IP 地址池 193.1.4.16/28,只允许内部网络终端发起访问外部网络(包括非军事区和非信任区)。

(2) 为防火墙配置的访问控制策略如下:

① 从信任区到非军事区:源 IP 地址=193.1.4.16/28,目的 IP 地址=193.1.2.5/32,HTTP 服务;

② 从信任区到非军事区:源 IP 地址=193.1.4.16/28,目的 IP 地址=193.1.2.6/32,SMTP+POP3 服务;

③ 从信任区到非信任区:源 IP 地址=193.1.4.16/28,目的 IP 地址=0.0.0.0,HTTP GET 服务;

④ 从非军事区到非信任区:源 IP 地址=193.1.2.6/32,目的 IP 地址=0.0.0.0,

SMTP 服务；

⑤ 从非信任区到非军事区：源 IP 地址＝0.0.0.0，目的 IP 地址＝193.1.2.5/32，HTTP GET 服务；

⑥ 从非信任区到非军事区：源 IP 地址＝0.0.0.0，目的 IP 地址＝193.1.2.6/32，SMTP 服务。

每一条访问控制策略给出三部分信息：一是信息流动方向，如策略 1 给出的从信任区到非军事区；二是允许启动信息交换过程的源终端地址范围和被动响应信息交换过程的目的终端地址范围，如策略 1 中允许启动信息交换过程的源终端是网络 193.1.4.16/28 内的任何终端，而允许被动响应信息交换过程的目的终端只能是 Web 服务器；三是以服务方式定义了整个信息交换过程。

(3) 路由器 R1 接口 2 输出方向设置如下分组过滤器：

permit 协议＝TCP，源 IP 地址＝192.168.1.0/24，目的 IP 地址＝192.168.2.3/32，目的端口号＝80；

permit 协议＝TCP，源 IP 地址＝192.168.1.0/24，目的 IP 地址＝192.168.2.7/32，目的端口号＝20；

permit 协议＝TCP，源 IP 地址＝192.168.1.0/24，目的 IP 地址＝192.168.2.7/32，目的端口号＝21；

deny 协议＝IP，源 IP 地址＝0.0.0.0/0，目的 IP 地址＝0.0.0.0/0。

(4) 网络入侵防御系统配置如表 2.2 所示。

表 2.2　网络入侵防御系统配置表

访问控制策略			攻击特征库	阈值和规则	反制动作
源 IP 地址	目的 IP 地址	服　务			
192.168.1.0/24	192.168.2.3/32	HTTP 服务	HTTP—严重	SYN 泛洪	丢弃
192.168.1.0/24	192.168.2.7/32	FTP 服务	FTP—严重	SYN 泛洪	丢弃

(5) 路由器 R1 接口 1 输入方向流量管制器

① 信息流分类标准：

协议＝TCP，源 IP 地址＝192.168.1.0/24，目的端口号＝25；

协议＝ICMP，源 IP 地址＝192.168.1.0/24。

② 流量：

平均＝3Mbps，峰值＝5Mbps。

2.3　实　　验

2.3.1　NAT 隐藏内部网络实验

1. 实验内容

(1) 内部网络设计和私有地址规划。

(2) 验证动态 NAT 工作机制。

(3) 完成路由器动态 NAT 配置。

(4) 验证私有地址与全球地址之间的转换过程。

(5) 验证内部网络隐藏过程。

2. 网络结构

网络结构如图 2.8 所示。对于路由器 R2 和 R3,内部网络(192.168.1.0/24 和 192.168.2.0/24)是透明的。为实现内部网络终端对外部网络的访问过程,对内部网络终端分配全球 IP 地址池 193.1.4.16/28,路由器 R2 和 R3 的路由表中给出用于指明通往网络 193.1.4.16/28 的传输路径的路由项,在内部网络终端发起访问外部网络后,由路由器 R1 建立内部网络私有地址和全球 IP 地址之间的绑定关系。只有在路由器 R1 建立内部网络私有地址和全球 IP 地址之间的绑定关系后,外部网络终端才能通过与内部网络私有地址绑定的全球 IP 地址和内部网络终端通信。

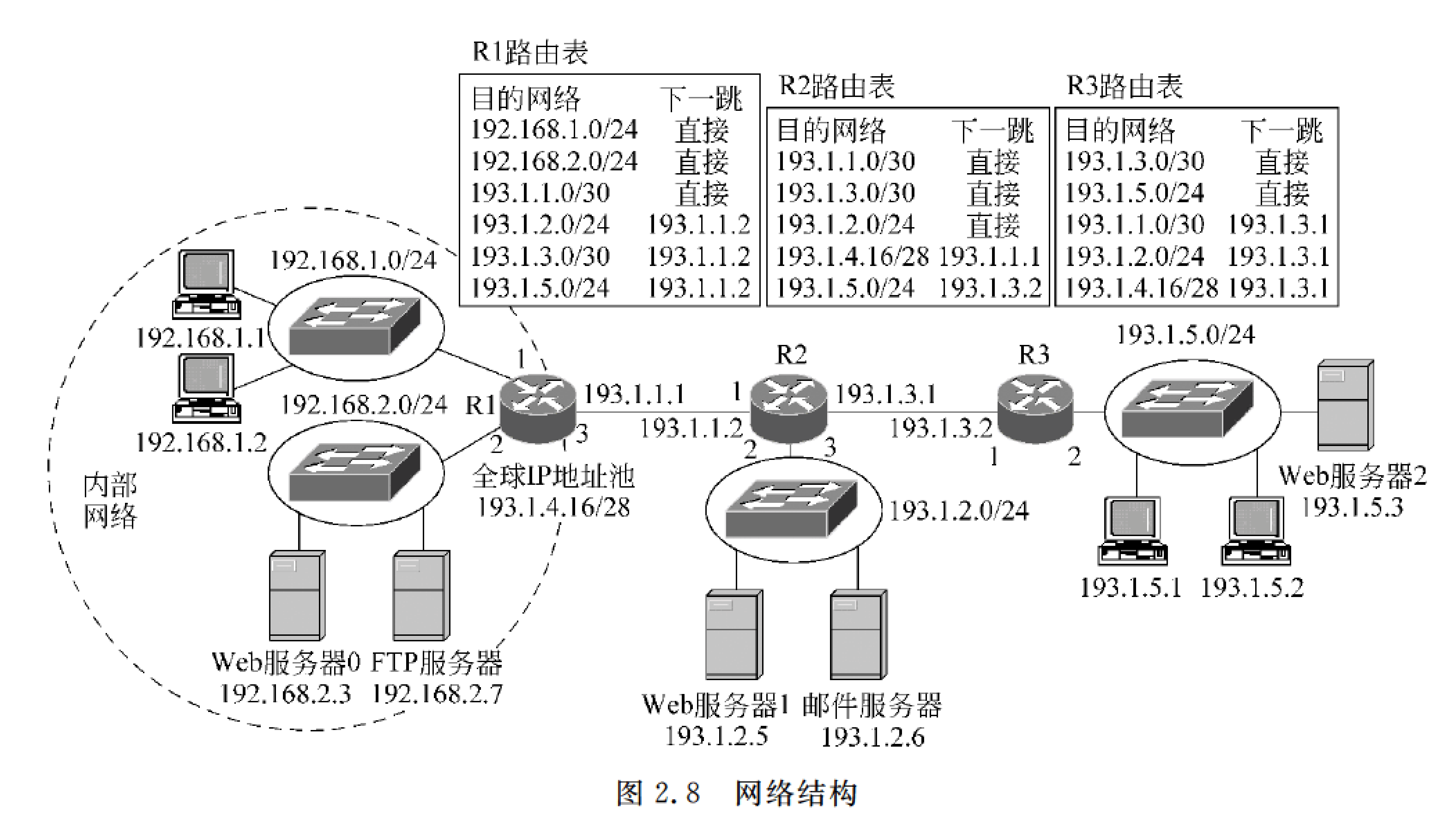


图 2.8 网络结构

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 2.8 所示的网络结构放置和连接设备,逻辑工作区完成设备放置和连接后的界面如图 2.9 所示。

(2) 对照图 2.8,完成图 2.9 中路由器 Router1、Router2 和 Router3 各个接口的 IP 地址和子网掩码配置,同时在路由器 Router1、Router2 和 Router3 中配置用于指明通往与其没有直接相连的网络的静态路由项。Router1 配置静态路由项的界面如图 2.10 所示。Router2 和 Router3 还需配置用于指明通往网络 193.1.4.16/28 的传输路径的静态路由项,193.1.4.16/28 是用于和私有网络地址 192.168.1.0/24 进行地址转换的全球 IP 地址池。各个路由器完成接口和静态路由项配置后的路由表如图 2.11～图 2.13 所示。需要指出的是,Router2 和 Router3 的路由表中并没有包含用于指明通往网络 192.168.1.0/24 和 192.168.2.0/24 的传输路径的路由项,内部网络对于其他网络中的终端是不

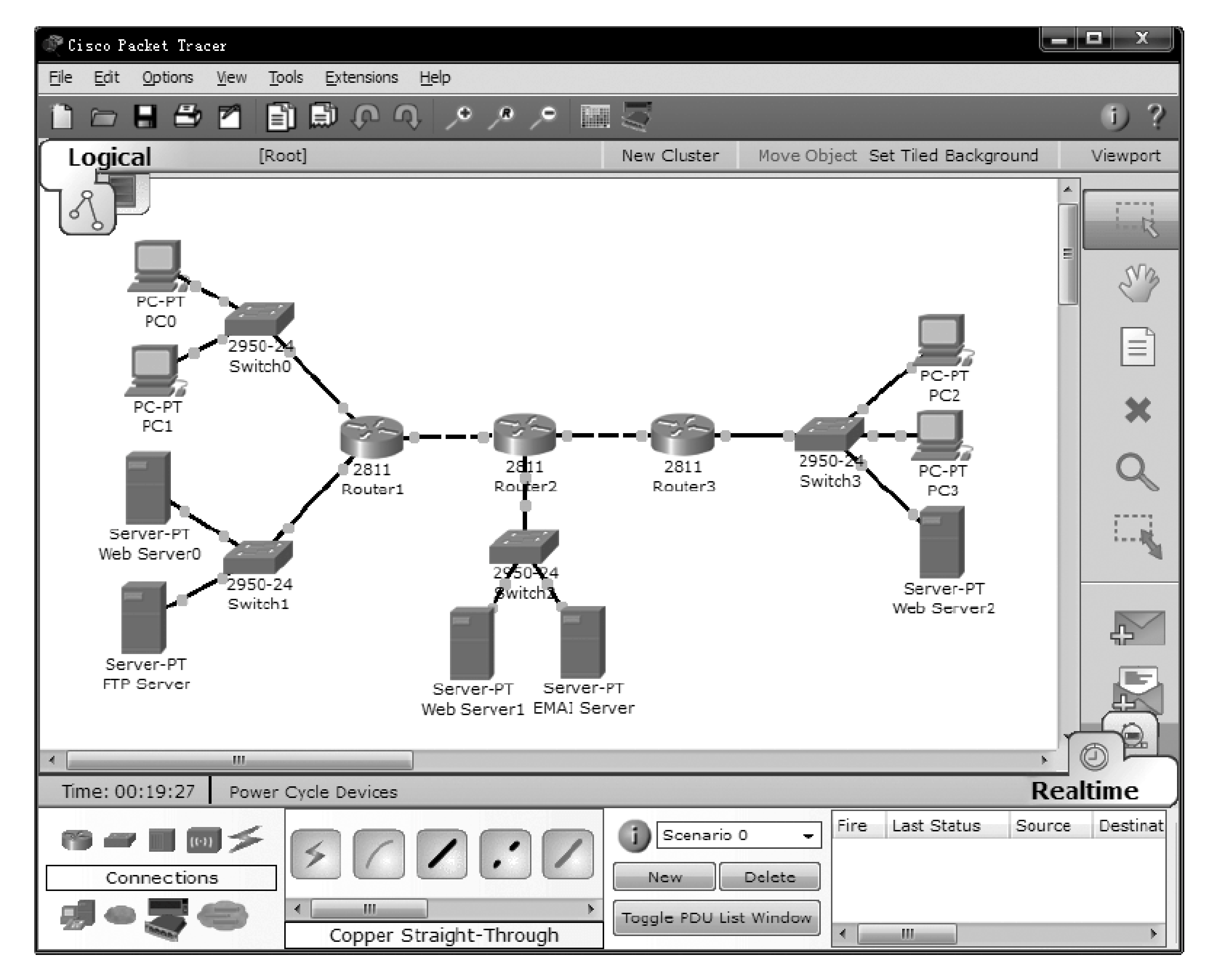


图 2.9　放置和连接设备后的逻辑工作区界面

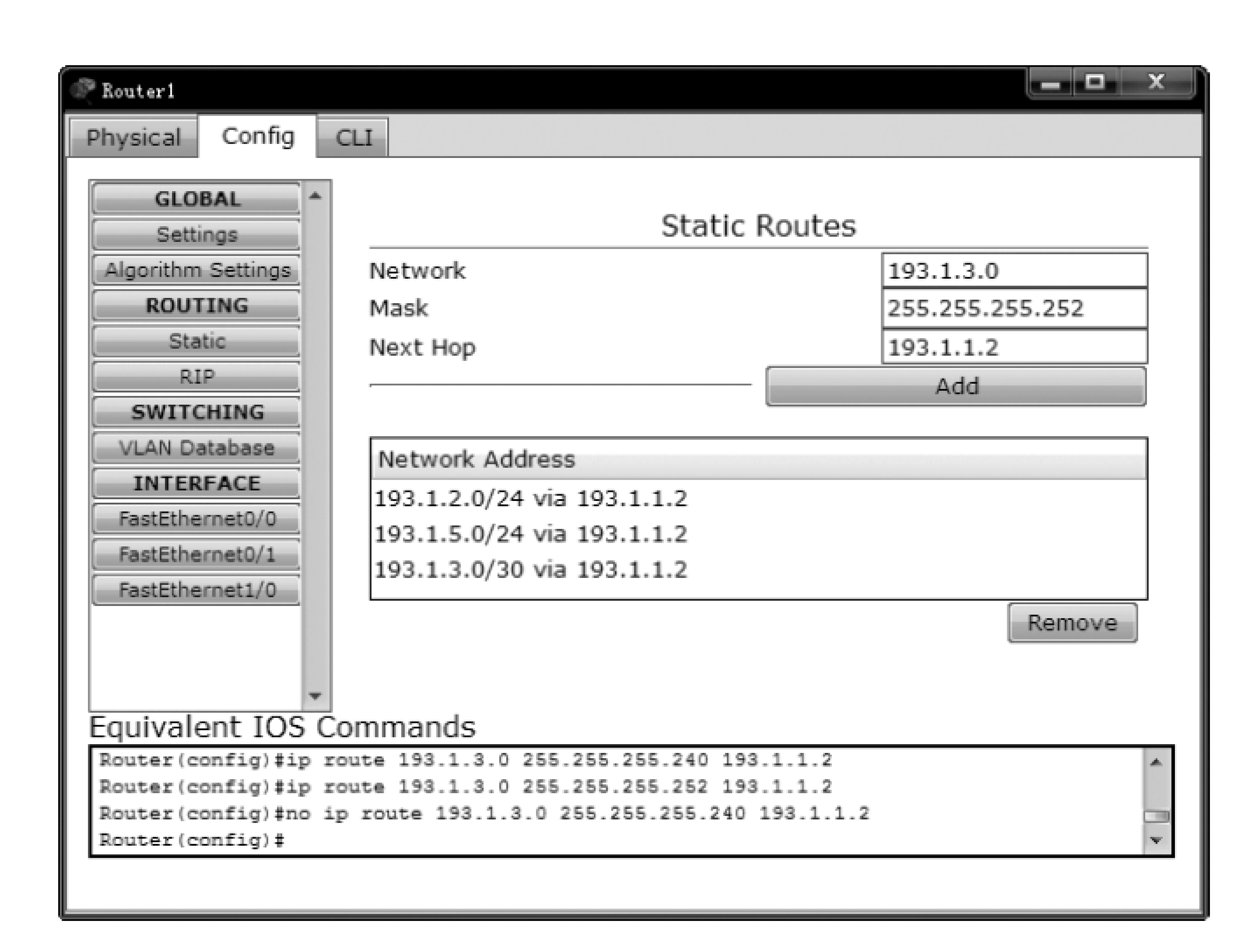


图 2.10　Router1 静态路由项配置界面

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0
C	193.1.1.0/30	FastEthernet1/0	---	0/0
S	193.1.2.0/24	---	193.1.1.2	1/0
S	193.1.3.0/30	---	193.1.1.2	1/0
S	193.1.5.0/24	---	193.1.1.2	1/0

图 2.11　Router1 路由表

Type	Network	Port	Next Hop IP	Metric
C	193.1.1.0/30	FastEthernet0/0	---	0/0
C	193.1.2.0/24	FastEthernet0/1	---	0/0
C	193.1.3.0/30	FastEthernet1/0	---	0/0
S	193.1.4.16/28	---	193.1.1.1	1/0
S	193.1.5.0/24	---	193.1.3.2	1/0

图 2.12 Router2 路由表

Type	Network	Port	Next Hop IP	Metric
C	193.1.3.0/30	FastEthernet0/0	---	0/0
C	193.1.5.0/24	FastEthernet0/1	---	0/0
S	193.1.1.0/30	---	193.1.3.1	1/0
S	193.1.2.0/24	---	193.1.3.1	1/0
S	193.1.4.16/28	---	193.1.3.1	1/0

图 2.13 Router3 路由表

可见的。

(3) 在路由器 Router1 中完成 NAT 配置,通过命令"ip nat pool 地址池名 起始 IP 地址 结束 IP 地址 netmask 子网掩码"定义全球 IP 地址池,如命令 ip nat pool a1 193.1.4.17 193.1.4.30 netmask 255.255.255.240 定义名为 a1、包含全球 IP 地址 193.1.4.17~193.1.4.30 的全球 IP 地址池。命令"access-list 编号 permit 网络地址 子网掩码反码"定义要求进行私有 IP 地址与全球 IP 地址转换的私有 IP 地址范围,编号的范围为 1~99,如命令 access-list 1 permit 192.168.1.0 0.0.0.255 要求对源 IP 地址属于 192.168.1.0/24 的 IP 分组进行 NAT 操作。命令"ip nat inside source list 编号 pool 地址池名"将私有 IP 地址范围与全球 IP 地址池绑定在一起,如命令 ip nat inside source list 1 pool a1。

(4) 在路由器 Router1 连接内部网络 192.168.1.0/24 的接口的配置过程中,通过命令"ip nat inside"确定该接口连接的网络是配置私有 IP 地址的内部网络,在连接外部网络的接口的配置过程中,通过命令"ip nat outside"确定该接口连接的网络是使用全球 IP 地址的外部网络。

(5) 按照图 2.8 所示的网络配置信息配置图 2.9 中各个终端和服务器的 IP 地址、子网掩码和默认网关地址。

(6) 完成终端 PC0、PC1 与 Web Server2 之间的 Ping 操作,Router1 中建立图 2.14 所示的网络地址转换(NAT)表。内部本地信息(Inside Local)是内部网络终端在内部网络中使用的信息,如内部网络终端发送的 ICMP ECHO 请求报文在内部网络中使用的本地源 IP 地址和本地标识符。内部全球信息(Inside Global)是内部网络终端在外部网络中使用的信息,如 ICMP ECHO 请求报文在外部网络中的全球源 IP 地址和标识符。外部本地信息(Outside Local)是外部网络终端在内部网络中使用的信息。外部全球信息(Outside Global)是外部网络终端在外部网络中使用的信息。除非外部网络地址范围和内部网络地址范围重叠,否则外部网络终端的这两种信息是相同的。完成终端 PC0、PC1 通过浏览器访问 Web Server2 过程,Router1 中建立图 2.15 所示的网络地址转换表。表中内部本地信息是该内部网络终端在内部网络中使用的源 IP 地址和源端口号,即本地源

IP 地址和源端口号。内部全球信息是地址转换后的源 IP 地址和源端口号，即全球源 IP 地址和源端口号。

NAT Table for Router1

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	193.1.4.17:1	192.168.1.1:1	193.1.5.3:1	193.1.5.3:1
icmp	193.1.4.18:1	192.168.1.2:1	193.1.5.3:1	193.1.5.3:1

图 2.14　完成 PC0、PC1 与 Web Server2 之间的 Ping 操作后的 Router1 NAT 表

NAT Table for Router1

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
tcp	193.1.4.18:1025	192.168.1.1:1025	193.1.5.3:80	193.1.5.3:80
tcp	193.1.4.19:1025	192.168.1.2:1025	193.1.5.3:80	193.1.5.3:80

图 2.15　PC0、PC1 用浏览器访问 Web Server2 后的 Router1 NAT 表

(7) 进入模拟操作模式，拦截 PC0 发送给 Web Server2 的 ICMP ECHO 请求报文，PC0 至 Router1 段的 IP 分组封装格式如图 2.16 所示，源 IP 地址是 PC0 的私有地址 192.168.1.1。Router1 至 Router2 段的 IP 分组封装格式如图 2.17 所示，源 IP 地址是全球 IP 地址池中的一个 IP 地址 193.1.4.20，由 Router1 完成私有 IP 地址至全球 IP 地址的转换。拦截 Web Server2 发送给 PC0 的 ICMP ECHO 响应报文，到达 Router1 之前的 IP 分组封装格式如图 2.18 所示，目的 IP 地址是全球 IP 地址 193.1.4.20。Router1 至 PC0 段的 IP 分组封装格式如图 2.19 所示，目的 IP 地址是 PC0 的私有地址 192.168.1.1，由 Router1 完成全球 IP 地址至私有 IP 地址的转换。

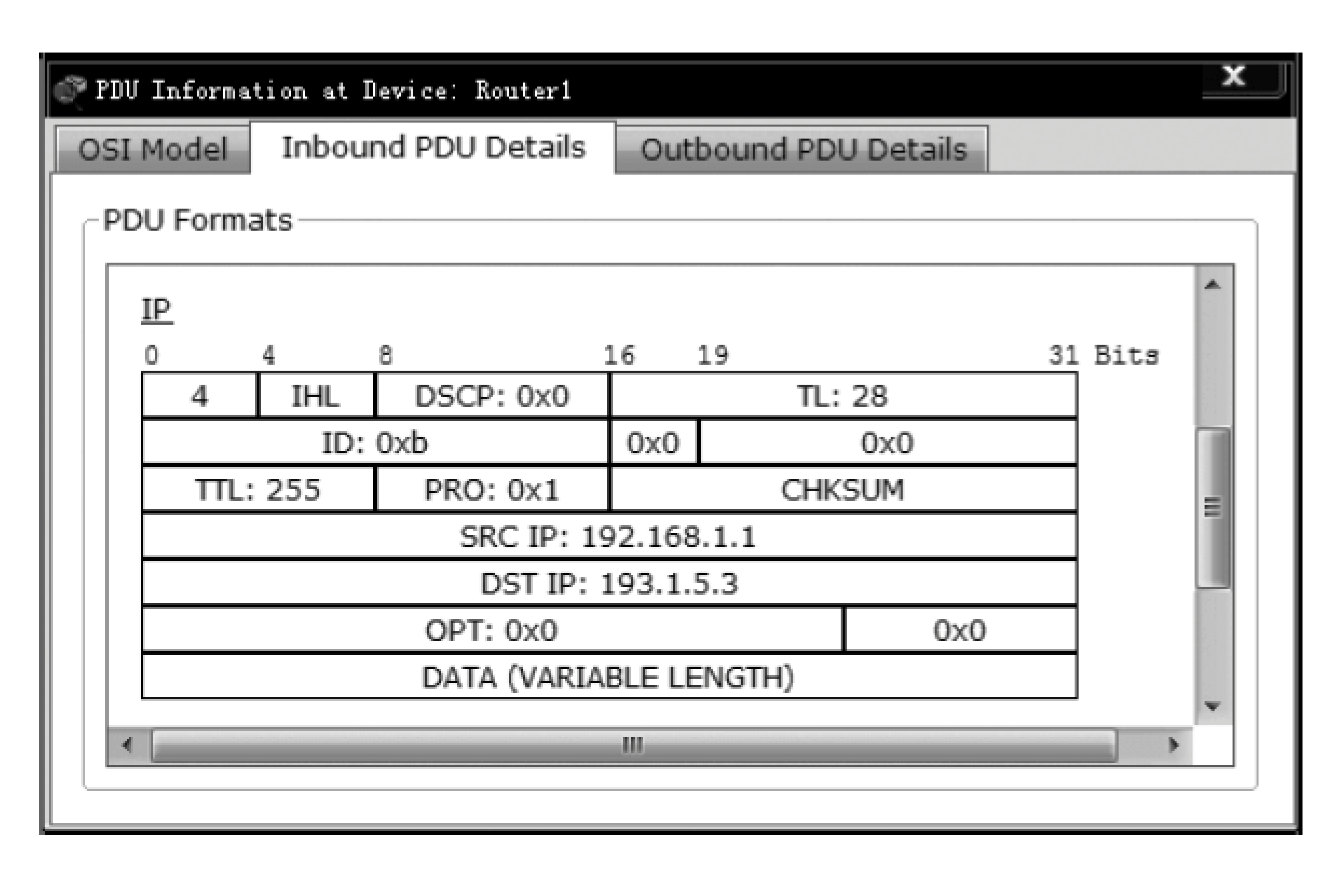


图 2.16　PC0→Web Server2 ICMP ECHO 请求报文 PC0 至 Router1 段 IP 分组封装格式

(8) 由于 Router1 NAT 配置中有两个特点，一是在访问控制列表中没有将内部网络地址 192.168.2.0/24 纳入需要进行 NAT 的源 IP 地址范围，二是没有在连接内部网络 192.168.2.0/24 的接口配置中通过命令“ip nat inside”将该接口连接的网络定义为需要 NAT 的内部网络。因此，Web Server0 发送给 Web Server2 的 ICMP ECHO 请求报文 Web Server0 至 Router1 段的 IP 分组封装格式如图 2.20 所示，源 IP 地址是 Web Server0

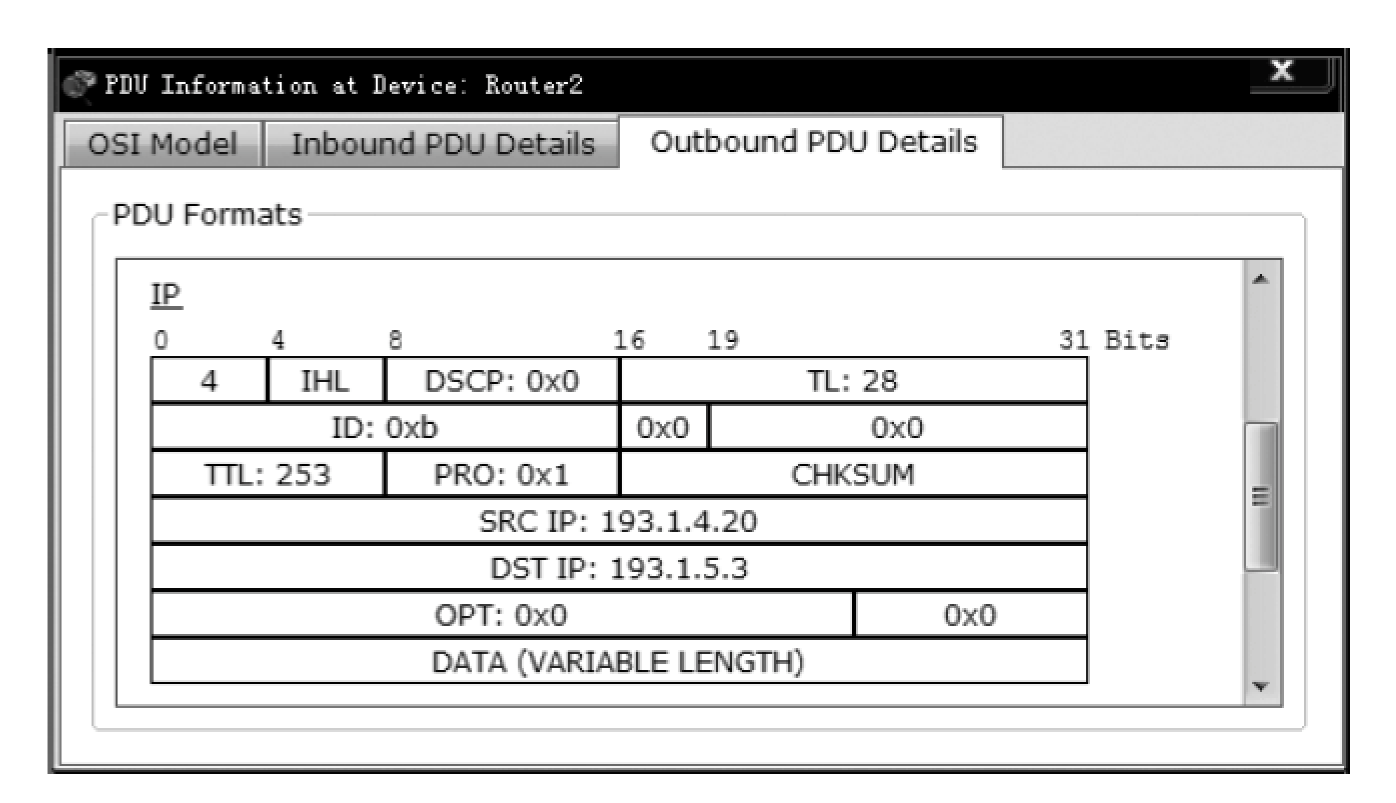


图 2.17 PC0→Web Server2 ICMP ECHO 请求报文 Router1 至 Router2 段 IP 分组封装格式

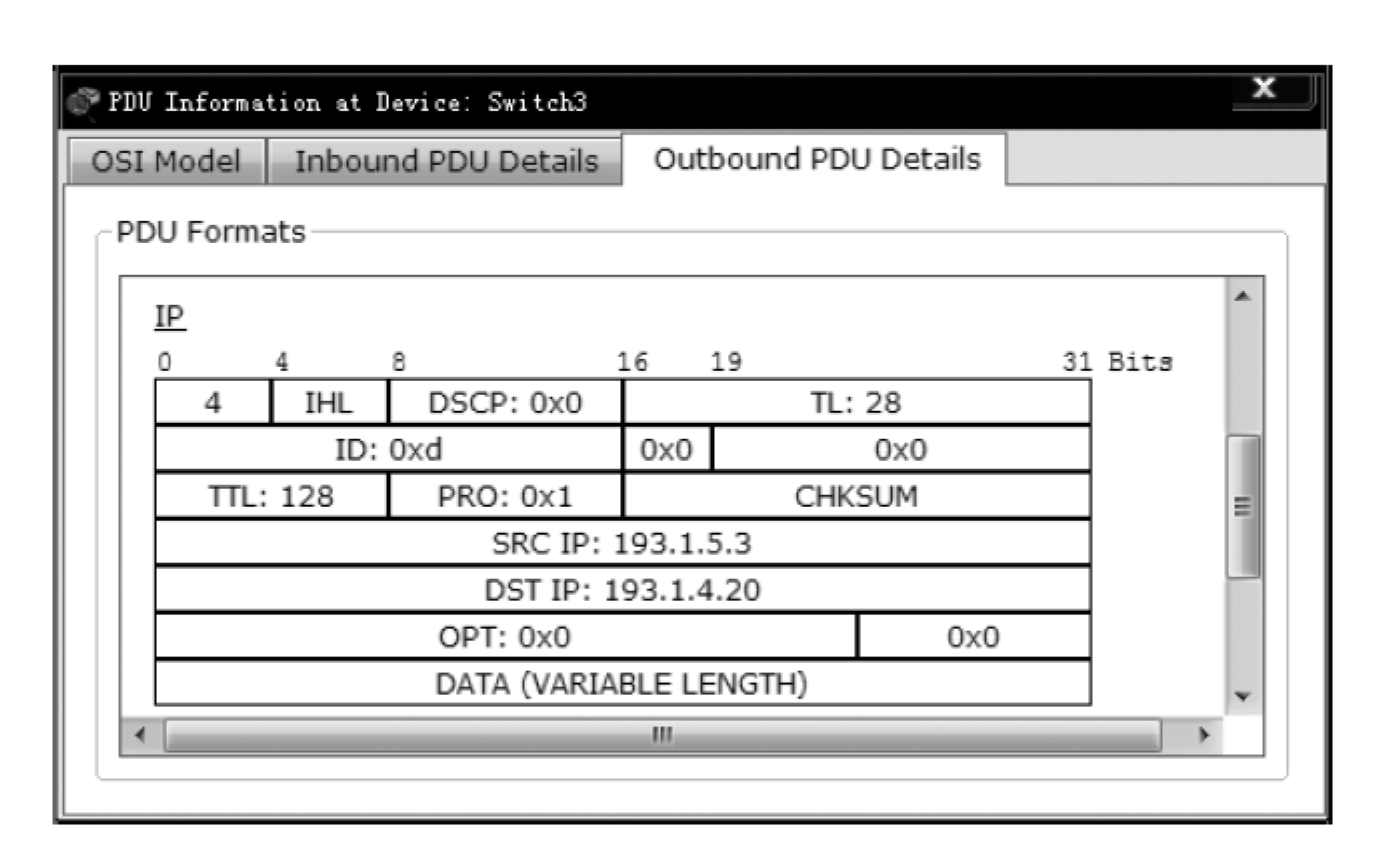


图 2.18 Web Server2→PC0 ICMP ECHO 响应报文 Web Server2 至 Router3 段 IP 分组封装格式

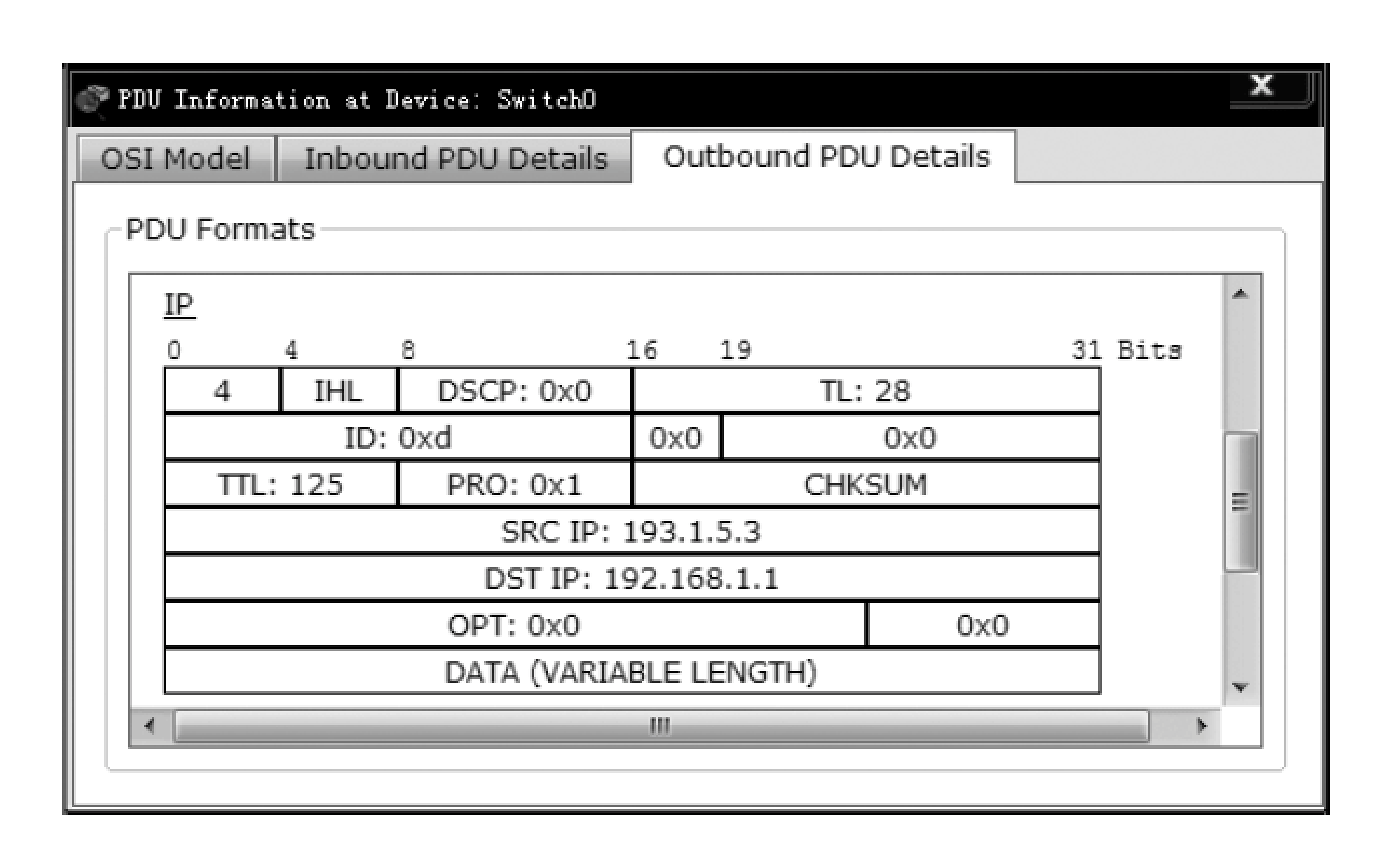


图 2.19 Web Server2→PC0 ICMP ECHO 响应报文 Router1 至 PC0 段 IP 分组封装格式

的私有 IP 地址 192.168.2.3，Router1 至 Router2 段的 IP 分组封装格式如图 2.21 所示，源 IP 地址仍然是 Web Server0 的私有 IP 地址 192.168.2.3。由于 Web Server2 发送给 Web Server0 的 ICMP ECHO 响应报文的目的 IP 地址是 Web Server0 的私有 IP 地址 192.168.2.3，如图 2.22 所示的 IP 分组封装格式。该 ICMP ECHO 响应报文由于没有在 Router3 的路由表中找到与目的地址 192.168.2.3 相匹配的路由项，被 Router3 丢弃。

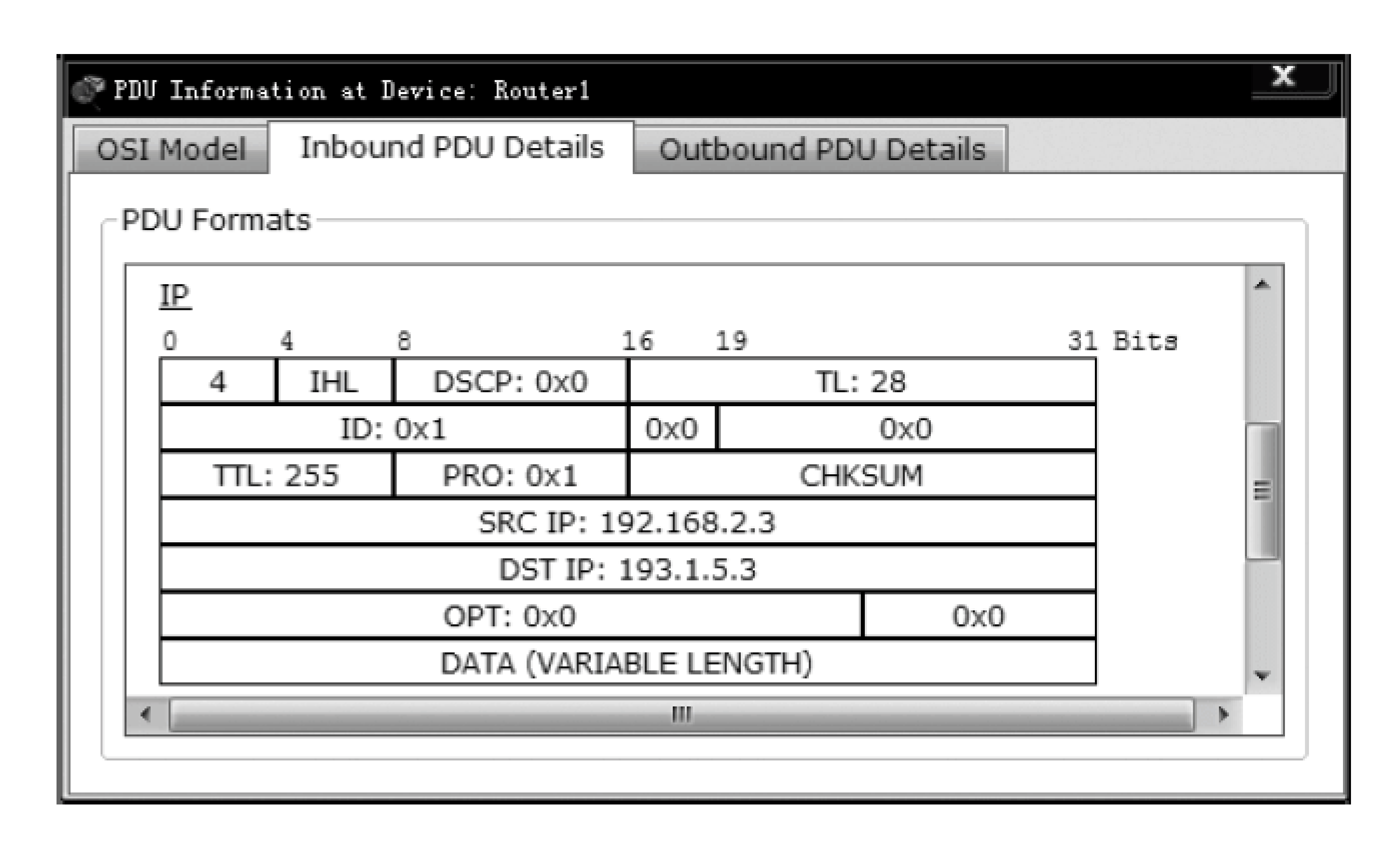


图 2.20　Web Server0→Web Server2 ICMP ECHO 请求报文 Web Server0 至 Router1 段 IP 分组封装格式

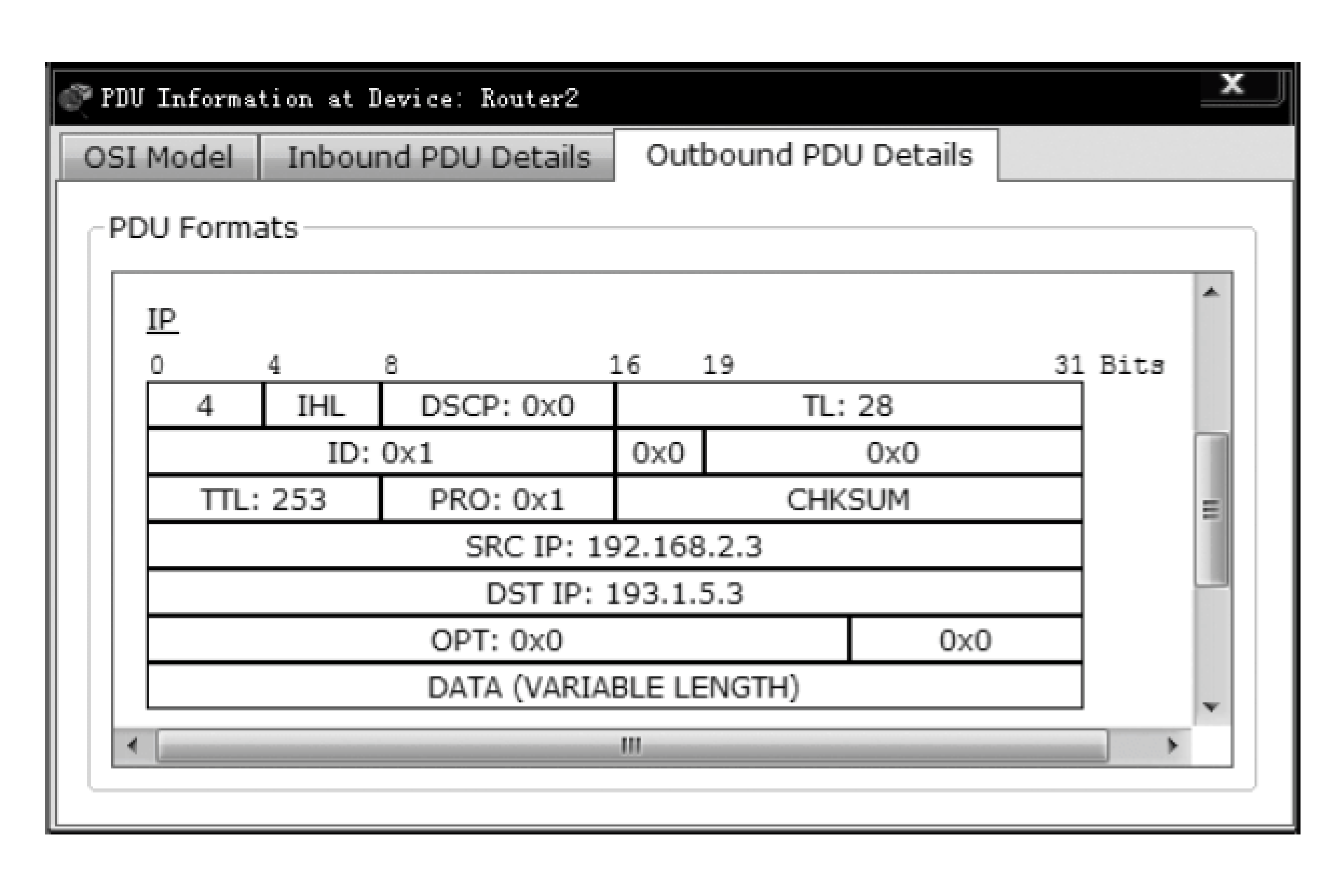


图 2.21　Web Server0→Web Server2 ICMP ECHO 请求报文 Router1 至 Router2 段 IP 分组封装格式

(9) 由于 Router3 和 Router2 只能路由以全球 IP 地址为目的地址的 IP 分组，因此必须在建立某个全球 IP 地址与某个内部网络终端的私有地址之间的绑定关系后，外部网络终端才能通过该全球 IP 地址访问与该全球 IP 地址绑定的内部网络终端。

4. Router1 命令行配置过程

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
```

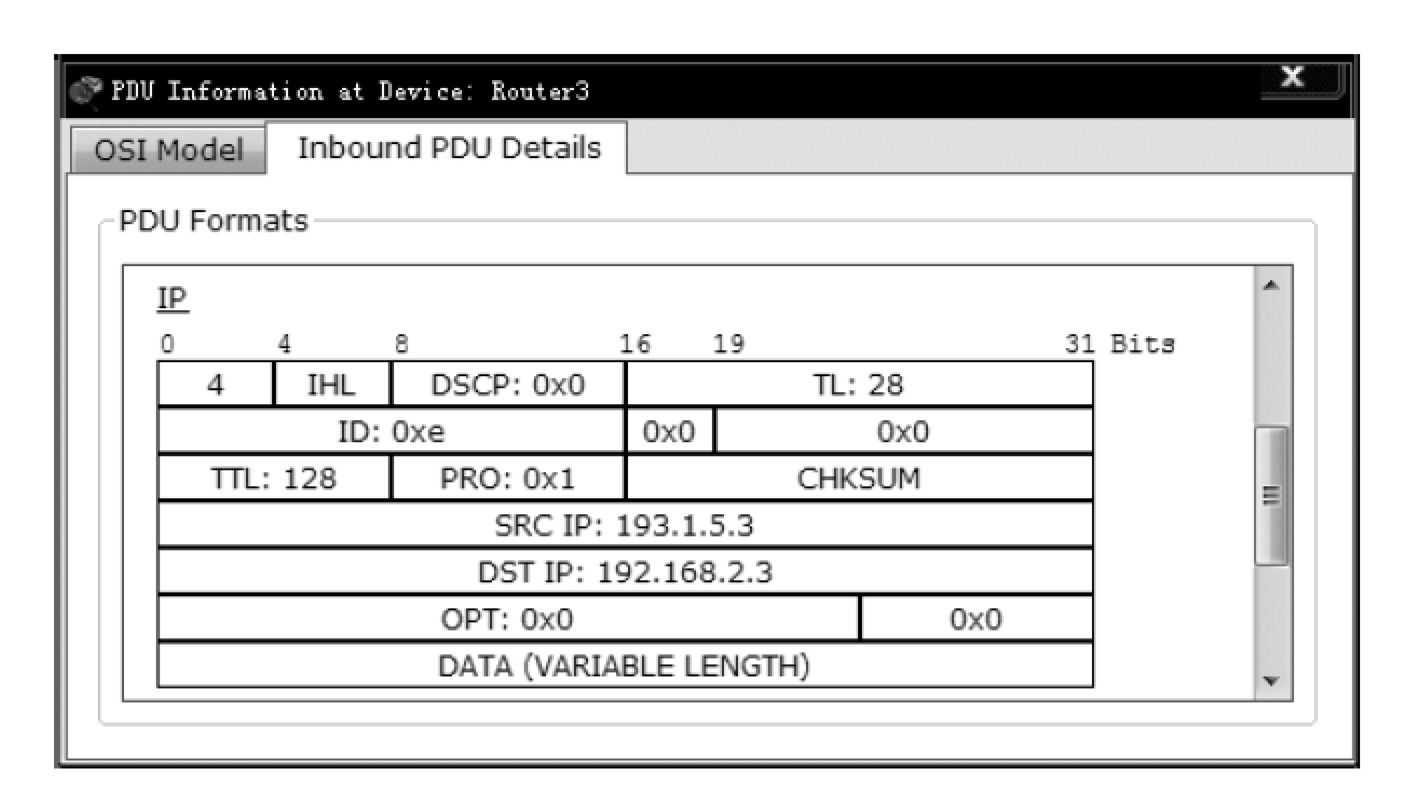


图 2.22　Web Server2 至 Web Server0 ICMP ECHO 响应报文 IP 分组封装格式

```
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 193.1.1.1 255.255.255.252
Router(config-if)#exit
Router(config)#ip route 193.1.2.0 255.255.255.0 193.1.1.2
                    (配置目的网络为 193.1.2.0/24,下一跳为 193.1.1.2 的静态路由项)
Router(config)#ip route 193.1.5.0 255.255.255.0 193.1.1.2
                    (配置目的网络为 193.1.5.0/24,下一跳为 193.1.1.2 的静态路由项)
Router(config)#ip route 193.1.3.0 255.255.255.252 193.1.1.2
                    (配置目的网络为 193.1.3.0/30,下一跳为 193.1.1.2 的静态路由项)
Router(config)#ip nat pool a1 193.1.4.17 193.1.4.30 netmask 255.255.255.240
    (建立包含 CIDR 地址块 193.1.4.16/28 中可用 IP 地址的全球 IP 地址池,a1 是该地址池的名字)
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
            (通过标准访问控制列表给出要求实现私有地址至全球 IP 地址转换的私有地址范围)
Router(config)#ip nat inside source list 1 pool a1
                    (将私有地址范围和全球 IP 地址池绑定在一起)
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside          (确定该接口连接配置私有地址的内部网络)
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip nat outside         (确定该接口连接配置全球 IP 地址的外部网络)
Router(config-if)#exit
```

Router2 和 Router3 除了缺少 NAT 配置外,其他命令行配置过程与 Router1 相似,

本书不再赘述。

2.3.2 有状态分组过滤器控制信息交换过程实验

1. 实验内容

（1）配置扩展分组过滤器。

（2）验证扩展分组过滤器的单向控制功能。

（3）配置有状态分组过滤器。

（4）验证有状态分组过滤器的双向控制功能。

（5）验证网络间分组传输控制过程。

2. 网络结构

该实验在 2.3.1 节 NAT 隐藏内部网络实验的基础上进行，要求在图 2.8 所示的路由器 R1 接口 2 输出方向上设置扩展分组过滤器，只允许与内部网络终端访问 Web 服务器 0 和 FTP 服务器相关的 TCP 报文进入网络 192.168.2.0/24。另外，通过配置有状态分组过滤器要求只允许内部网络 192.168.1.0/24 中的终端发起访问 Web 服务器 1 和 Web 服务器 2，禁止其他内部网络与外部网络之间的信息交换过程。

3. 实验步骤

（1）实现只允许与内部网络终端访问 Web Server0 和 FTP Server 相关的 TCP 报文进入网络 192.168.2.0/24 的访问控制的扩展分组过滤器如下：

```
access-list 101 permit tcp 192. 168.1.0 0.0.0.255 192.168.2.3 0.0.0.0 eq 80
access-list 101 permit tcp 192. 168.1.0 0.0.0.255 192.168.2.7 0.0.0.0 eq 21
access-list 101 permit tcp 192. 168.1.0 0.0.0.255 192.168.2.7 0.0.0.0 eq 20
access-list 101 deny ip any any
```

编号 100～199 表明是扩展分组过滤器。①过滤规则表明允许源 IP 地址为 192.168.1.0/24，源端口号任意，目的 IP 地址为 192.168.2.3/32，目的端口号为 80 的 TCP 报文正常转发。192.168.1.0 0.0.0.255 表示源 IP 地址的范围，即和 192.168.1.0 高 24 位相同的 IP 地址集合，等同于网络地址 192.168.1.0/24 表示的 IP 地址范围。可以将 0.0.0.255 看作是子网掩码 255.255.255.0 的反码。192.168.2.3 0.0.0.0 表示主机地址 192.168.2.3/32，可以用 host 192.168.2.3 代替。

在接口配置模式下，通过命令 ip access-group 101 out 将编号为 101 的扩展分组过滤器作用到路由器 Router1 接口 FastEthernet0/1 的输出方向上。完成配置后，属于网络 192.168.1.0/24 的终端可以通过浏览器访问 Web Server0，如图 2.23 所示。但不能向 Web Server0 发送目的端口号不等于 80 的 TCP 报文和其他类型的报文，如图 2.24 所示的 ICMP 报文。

（2）在 Router2 配置实现只允许内部网络 192.168.1.0/24 中的终端发起访问 Web Server1 和 Web Server2 的访问控制的有状态分组过滤器的步骤如下：

① 在路由器 Router2 接口 FastEthernet0/0 的输入方向上设置实现只允许与内部网络 192.168.1.0/24 中的终端访问 Web Server1 和 Web Server2 有关的 TCP 报文沿着内部网络至网络 193.1.2.0/24 和网络 193.1.5.0/24 方向传输的访问控制的扩展分组过滤器。

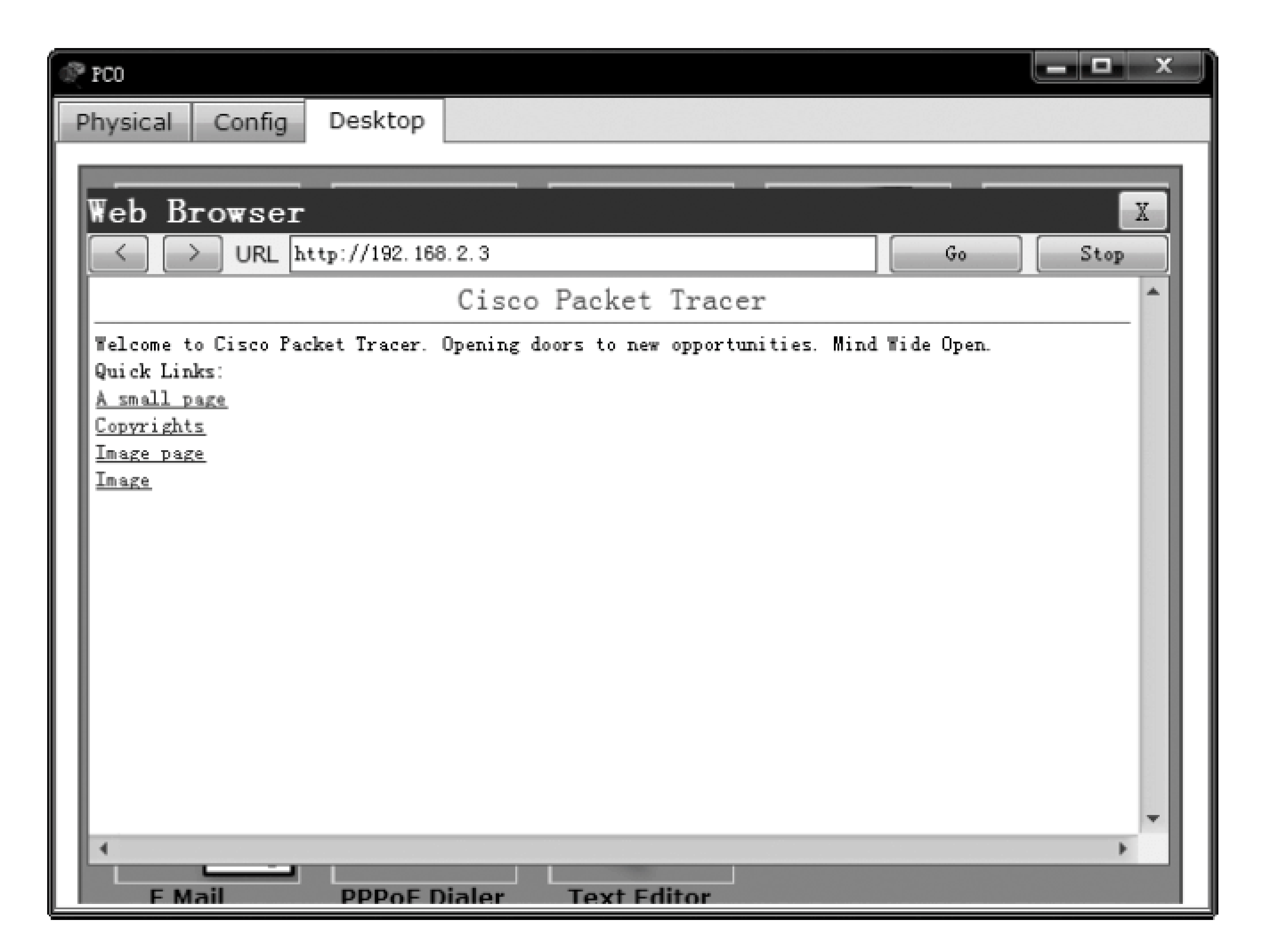


图 2.23 PC0 访问 Web Server0 的界面

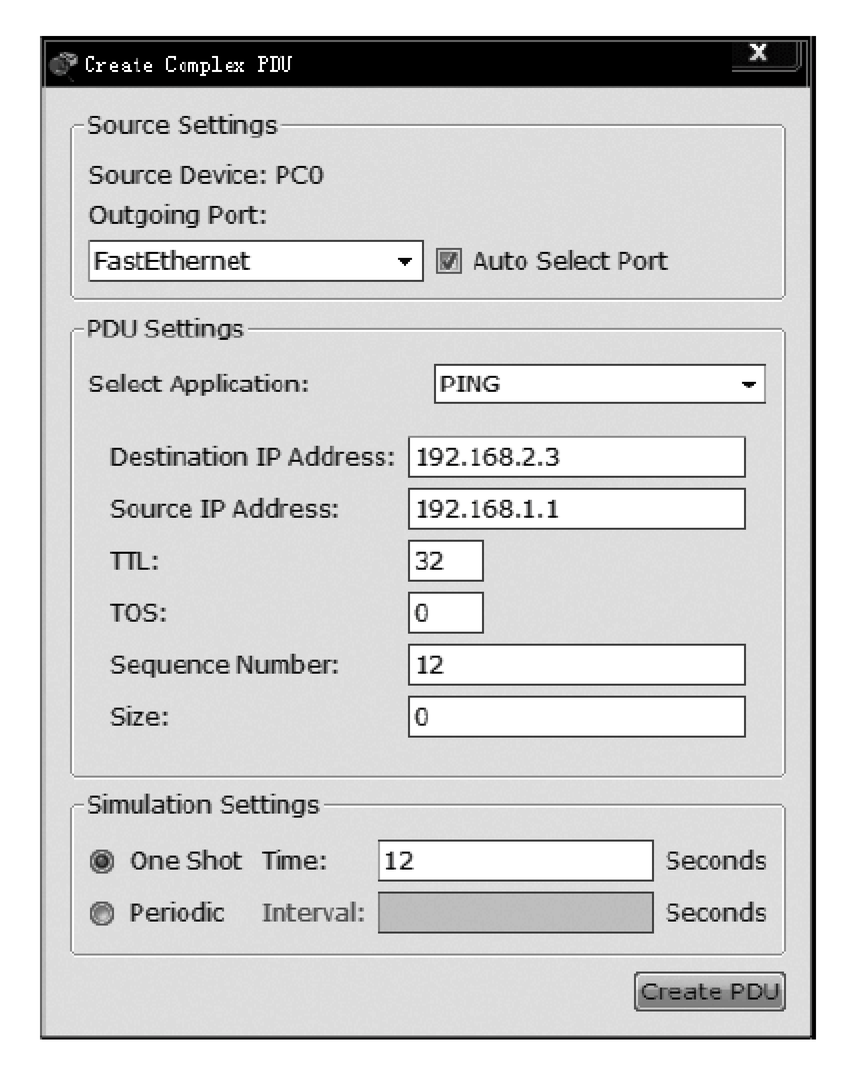


图 2.24 PC0 至 Web Server0 的 ICMP 报文

```
access-list 101 permit tcp 193.1.4.16 0.0.0.15 193.1.2.5 0.0.0.0 eq 80
access-list 101 permit tcp 193.1.4.16 0.0.0.15 193.1.5.3 0.0.0.0 eq 80
access-list 101 deny ip any any
```

193.1.4.16 0.0.0.15 表示源 IP 地址范围 193.1.4.16/28,0.0.0.15 是子网掩码 255.255.255.240 的反码。

在路由器 Router2 接口 FastEthernet0/1 输出方向上设置实现只允许与内部网络 192.168.1.0/24 中的终端访问 Web Server1 有关的 TCP 报文沿着内部网络至网络 193.1.2.0/24 方向传输的访问控制的扩展分组过滤器。

```
access-list 103 permit tcp 193.1.4.16 0.0.0.15 193.1.2.5 0.0.0.0 eq 80
access-list 103 deny ip any any
```

在路由器 Router2 接口 FastEthernet1/0 输出方向上设置实现只允许与内部网络 192.168.1.0/24 中的终端访问 Web Server2 有关的 TCP 报文沿着内部网络至网络 193.1.5.0/24 方向传输的访问控制的扩展分组过滤器。

```
access-list 104 permit tcp 193.1.4.16 0.0.0.15 193.1.5.3 0.0.0.0 eq 80
access-list 104 deny ip any any
```

② 在相反方向配置禁止一切 IP 分组传输的扩展分组过滤器。

```
access-list 102 deny ip any any
```

③ 沿着内部网络至网络 193.1.2.0/24 方向和内部网络至网络 193.1.5.0/24 方向配置实现有状态分组过滤器的检查规则。

```
ip inspect name a3 http
```

它表明一旦沿着内部网络至网络 193.1.2.0/24 方向和内部网络至网络 193.1.5.0/24 方向传输了与内部网络 192.168.1.0/24 中的终端访问 Web Server1 和 Web Server2 有关的 TCP 报文，包括建立 TCP 连接请求报文和 HTTP 请求报文，必须在相反方向动态配置允许对应的响应报文沿着网络 193.1.2.0/24 和 193.1.5.0/24 至内部网络方向传输的过滤规则。这就是有状态分组过滤器的本质，根据当前的会话状态确定完成下一阶段工作需要交换的报文类型，只允许完成下一阶段工作需要的报文交换过程进行。

(3) 用和(2)相似的步骤完成 Router3 访问控制策略配置。完成配置后，属于网络 192.168.1.0/24 的终端可以通过浏览器访问 Web Server1 和 Web Server2，PC0 访问 Web Server1 的界面如图 2.25 所示。

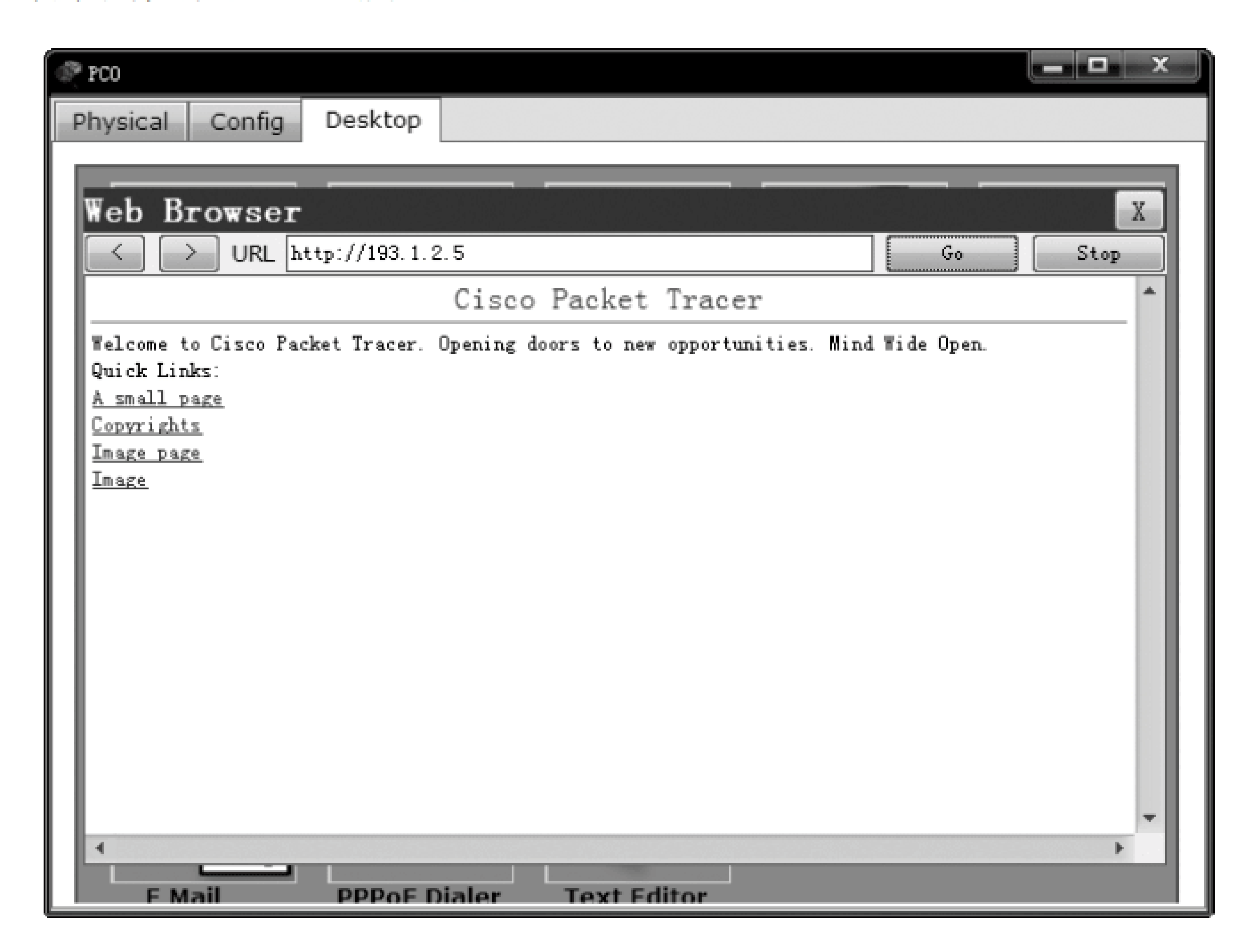


图 2.25　PC0 访问 Web Server1 界面

(4) 进入模拟操作模式,在 Web Server2 创建一个目的 IP 地址为 193.1.4.20 的 HTTP 报文,如图 2.26 所示。该 HTTP 报文在路由器 Router3 被分组过滤器丢弃。可以确定,除了内部网络终端访问 Web Server1 和 Web Server2 的过程能够正常进行外,禁止其他一切内部网络和外部网络之间的信息交换过程。

图 2.26 Web Server2 至 PC0 的 HTTP 报文

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.3 0.0.0.0 eq 80
                              (该过滤规则表明允许源 IP 地址为 192.168.1.0/24,源端口号任意,目的
                               IP 地址为 192.168.2.3/32,目的端口号为 80 的 TCP 报文正常转发)
Router(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.7 0.0.0.0 eq 21
                              (该过滤规则表明允许源 IP 地址为 192.168.1.0/24,源端口号任意,目的
                               IP 地址为 192.168.2.7/32,目的端口号为 21 的 TCP 报文正常转发)
Router(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.7 0.0.0.0 eq 20
                              (该过滤规则表明允许源 IP 地址为 192.168.1.0/24,源端口号任意,目的
                               IP 地址为 192.168.2.7/32,目的端口号为 20 的 TCP 报文正常转发)
Router(config)#access-list 101 deny ip any any    (该过滤规则拒绝其他一切 IP 分组)
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 101 out
                        (将编号为 101 的扩展分组过滤器作用于接口 FastEthernet0/1 输出方向)
Router(config-if)#exit
```

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#access-list 101 permit tcp 193.1.4.16 0.0.0.15 193.1.2.5 0.0.0.0 eq 80
                    (该过滤规则表明允许源 IP 地址为 193.1.4.16/28,源端口号任意,目的
                    IP 地址为 193.1.2.5/32,目的端口号为 80 的 TCP 报文正常转发)
Router(config)#access-list 101 permit tcp 193.1.4.16 0.0.0.15 193.1.5.3 0.0.0.0 eq 80
                    (该过滤规则表明允许源 IP 地址为 193.1.4.16/28,源端口号任意,目的
                    IP 地址为 193.1.5.3/32,目的端口号为 80 的 TCP 报文正常转发)
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 deny ip any any
Router(config)#access-list 103 permit tcp 193.1.4.16 0.0.0.15 193.1.2.5 0.0.0.0 eq 80
                    (该过滤规则表明允许源 IP 地址为 193.1.4.16/28,源端口号任意,目的
                    IP 地址为 193.1.2.5/32,目的端口号为 80 的 TCP 报文正常转发)
Router(config)#access-list 103 deny ip any any
Router(config)#ip inspect name a2 http
                 (创建名为 a2 的检查规则,如果是访问 Web 服务器相关的 TCP 报文,则在
                 相反方向动态建立允许该 TCP 报文对应的响应报文正常转发的过滤
规则)
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 101 in
                 (将编号为 101 的扩展分组过滤器作用于接口 FastEthernet0/0 输入方向)
Router(config-if)#ip access-group 102 out
                 (将编号为 102 的扩展分组过滤器作用于接口 FastEthernet0/0 输出方向)
Router(config-if)#ip inspect a2 in
               (将名为 a2 的检查规则作用于接口 FastEthernet0/0 输入方向。一旦输入方向
               检查到与访问 Web 服务器相关的 TCP 报文,则在输出方向动态设置允许该 TCP
               报文对应的响应报文进入接口 FastEthernet0/0 连接的网络的过滤规则)
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 103 out
Router(config-if)#ip access-group 102 in
Router(config-if)#ip inspect a2 out
Router(config-if)#exit
Router(config)#access-list 104 permit tcp 193.1.4.16 0.0.0.15 193.1.5.3 0.0.0.0 eq 80
                    (该过滤规则表明允许源 IP 地址为 193.1.4.16/28,源端口号任意,目的
                    IP 地址为 193.1.5.3/32,目的端口号为 80 的 TCP 报文正常转发)
Router(config)#access-list 104 deny ip any any
Router(config)#interface FastEthernet1/0
Router(config-if)#ip access-group 104 out
Router(config-if)#ip inspect a2 out
Router(config-if)#ip access-group 102 in
Router(config-if)#exit
```

(3) Router3 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#access-list 101 permit tcp 193.1.4.16 0.0.0.15 193.1.5.3 0.0.0.0 eq 80
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 deny ip any any
Router(config)#ip inspect name a2 http
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#ip inspect a2 in
Router(config-if)#ip access-group 102 out
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 101 out
Router(config-if)#ip inspect a2 out
Router(config-if)#ip access-group 102 in
Router(config-if)#exit
```

2.3.3 流量管制器抑制病毒传播实验

1. 实验内容

(1) 配置流量管制器。

(2) 限制特定信息流的流量。

(3) 通过流量管制抑制病毒传播。

2. 网络结构

网络结构如图 2.8 所示。为了抑制电子邮件病毒的传播，需要限制内部网络 192.168.1.0/24 和外部网络 193.1.5.0/24 中终端通过 SMTP 向邮件服务器发送邮件的流量。流量管制器一是需要配置分类器，通过分类器指定信息流；二是需要配置和速率限制有关的两个参数，即平均速率(Xbps)和突发长度(YB)，令牌生成器以平均速率向令牌桶放入令牌，时间段 T 产生的令牌为 $T\times X/8$(B)，令牌桶的深度为 Y(单位为 B)，当放入的令牌超过 Y 时，后续令牌将被丢弃。实际配置中令牌桶深度为规定时间段 TC 放入的令牌(令牌桶深度为 $TC\times X/8$(B))，因此配置了平均速率后，即配置了令牌桶深度。在令牌桶中令牌为 P(B)时，如果到达一个长度为 Z(B)且 $Z\leqslant P$ 的分组，表明分组到达速率遵守规定速率，分组正常传输，$P=P-Z$。如果到达一个长度为 Z(B)且 $Z>P$ 的分组，分组在输出队列中等待，直到令牌桶中令牌 $P\geqslant Z$，以此限制特定信息流的流量。这里通过分组过滤器指定特定信息流，指定与内部网络 192.168.1.0/24 中终端通过 SMTP 向邮件服务器发送邮件相关的信息流的分组过滤器如下：

```
permit tcp 192.168.1.0 0.0.0.255 193.1.2.6 0.0.0.0 eq smtp
deny ip any any
```

指定与外部网络 193.1.5.0/24 中终端通过 SMTP 向邮件服务器发送邮件相关的信

息流的分组过滤器如下：

```
permit tcp 193.1.5.0 0.0.0.255 193.1.2.6 0.0.0.0 eq smtp
deny ip any any
```

限制流量的配置命令如下：

```
shape average 8000
```

8000 是平均速率，单位为 bps。

在图 2.8 所示的路由器 R1 接口 3 中设置用于限制内部网络 192.168.1.0/24 中终端通过 SMTP 向邮件服务器发送邮件的流量的流量管制器，在图 2.8 所示的路由器 R3 接口 1 中设置用于限制外部网络 193.1.5.0/24 中终端通过 SMTP 向邮件服务器发送邮件的流量的流量管制器。

3. 命令行配置过程

（1）Router1 命令行配置过程。

```
Router(config)#access-list 106 permit tcp 192.168.1.0 0.0.0.255 193.1.2.6 0.0.0.0 eq smtp
                                        (设置用于指定内部网络 192.168.1.0/24 中终端通过
                                         SMTP 向邮件服务器发送邮件的信息流的过滤规则)
Router(config)#access-list 106 deny ip any any
Router(config)#class-map email          (打开分类器配置过程,email 是分类器名称)
Router(config-cmap)#match access-group 106
                                         (指定分类标准是编号为 106 的分组过滤器)
Router(config-cmap)#exit
Router(config)#policy-map email         (打开流量管制器配置过程)
Router(config-pmap)#class email         (设置与流量管制器关联的分类器)
Router(config-pmap-c)#shape average 8000    (设置平均速率为 8000bps)
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#service-policy output email
                  (将名为 email 的流量管制器配置到 Router1 FastEthernet1/0 接口的输出方向)
Router(config-if)#exit
```

（2）Router3 命令行配置过程。

```
Router(config)#access-list 106 permit tcp 193.1.5.0 0.0.0.255 193.1.2.6 0.0.0.0 eq smtp
                                        (设置用于指定外部网络 193.1.5.0/24 中终端通过
                                         SMTP 向邮件服务器发送邮件的信息流的过滤规则)
Router(config)#access-list 106 deny ip any any
Router(config)#class-map email
Router(config-cmap)#match access-group 106
Router(config-cmap)#exit
Router(config)#policy-map email
Router(config-pmap)#class email
```

```
Router(config-pmap-c)#shape average 8000
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#service-policy output email
Router(config-if)#exit
```

第3章 黑客攻击机制

CHAPTER

3.1 知识要点

3.1.1 黑客攻击对象

网络由主机系统、转发结点和链路组成，将转发结点和实现转发结点互连的链路称为网络设施，因此，黑客攻击对象也分为主机系统和网络设施。

1. 主机系统

主机系统中存储了大量的信息资源，黑客攻击主机系统的主要目标是非法获取存储在主机系统中的信息资源，黑客非法获取主机系统中信息资源的过程称为非法访问，网络使得远程非法访问成为了可能。由于远程非法访问的隐蔽性和方便性，使得远程非法访问成为黑客攻击主机系统的主要手段。由于主机系统是网络的主要服务提供者，黑客攻击主机系统的另一个目的是使主机系统丧失服务功能。

2. 网络设施

转发结点中的配置信息、控制信息直接影响数据传输过程，因此，黑客攻击网络设施的重要目标是能够侵入转发结点，篡改配置信息和控制信息，使数据传输过程按照黑客预期的方向进行。传输过程中的信息资源是网络信息资源的重要组成部分，黑客攻击网络设施的另一个目标是嗅探、截获传输过程中的信息资源。实现正常的端到端数据传输是保障网络服务的基础，黑客攻击网络设施的又一个目标是破坏网络正常的端到端数据传输功能。

3.1.2 黑客攻击手段

1. 主机系统攻击手段

使主机系统感染病毒是最常见的主机系统攻击手段，病毒可以使主机系统按照黑客要求外泄信息，允许黑客随时登录主机系统，根据黑客指令对主机系统实施破坏。狭义病毒和蠕虫感染主机系统的方法已在第 2 章

做了详细讨论。利用主机系统漏洞非法登录主机系统，对主机系统资源实施非法访问，甚至上传病毒和木马，以此实现对该主机系统的长期控制仍然是黑客针对特定主机系统的主要攻击手段。黑客对特定主机系统的攻击过程分为侦查、扫描、获取访问权限、保持访问权限和消除入侵痕迹5个步骤。

(1) 侦查。

获取有关特定主机系统的信息，如域名、IP地址和所属单位的组织结构等。

(2) 扫描。

通过Ping操作确定主机系统是否在线，通过端口扫描确定主机系统打开的服务，通过探测过程确定主机操作系统类型及版本，通过漏洞扫描发现主机操作系统或应用程序存在的漏洞。

(3) 获取访问权限(缓冲器溢出和弱口令)。

通过猜测口令和字典文件破解弱口令。弱口令是指由一组关联性较强的字符组成的口令，如员工姓名全拼音、单位名称中每个汉字拼音的首个字符组合以及某个标准英语单词等。通过精心设计字典文件可以比较容易地破解弱口令。

通过利用操作系统或应用程序漏洞实施非法登录，最常见的操作系统或应用程序漏洞是缓冲器溢出，利用缓冲器溢出可以在主机上运行黑客的shellcode，并因此实现非法登录。

(4) 保持访问权限。

一旦实现非法登录，黑客或者创建具有管理员权限的账户，或者上传木马，在主机上保留后门，以便下次登录。

(5) 消除入侵痕迹。

为了隐藏入侵过程，往往需要在日志文件中删除和本次入侵过程相关的事件。

2. 网络设施攻击手段

网络设施攻击手段主要有信息嗅探攻击、信息拦截攻击、拒绝服务攻击、路由项欺骗攻击、DHCP欺骗攻击、DNS欺骗攻击、非法接入、重放攻击、分布式拒绝服务攻击和网络设备侵入等，大部分攻击手段已经在第1章的1.4节实验中作了详细讨论。

3.1.3 黑客攻击防御机制

1. 加密、完整性检测和鉴别

加密可以防止信息窃取，完整性检测可以防止信息篡改，源端鉴别可以防止源IP地址欺骗，身份鉴别可以防止非法访问。

2. 主机入侵防御系统

主机入侵防御系统是保护主机系统免遭攻击的主要手段，通过资源访问控制和行为监管，可以有效防御未知病毒实施的破坏操作和黑客对主机系统的攻击。

3. 网络入侵防御系统

无论是发生对主机系统的攻击行为，还是对网络设施的攻击行为，都会引发信息流异常，通过检测流经关键网段的信息流，可以发现正在实施的攻击，并加以干预。

4. 接入控制和交换机端口配置

安全端口使得每一个端口与一组 MAC 地址绑定，只有源 MAC 地址属于这组 MAC 地址的 MAC 帧才能通过该端口输入并转发。如图 3.1 所示，交换机端口之间或交换机端口与终端之间接入集线器，一方面使得黑客终端可以通过集线器嗅探两个交换机之间传输的信息，另一方面可以使得黑客终端通过假冒授权终端的 MAC 地址绕过安全端口的接入控制过程，非法接入网络。因此，必须通过配置，强迫交换机端口工作在全双工通信方式，保证交换机端口之间、交换机端口与终端之间无法接入集线器设备。

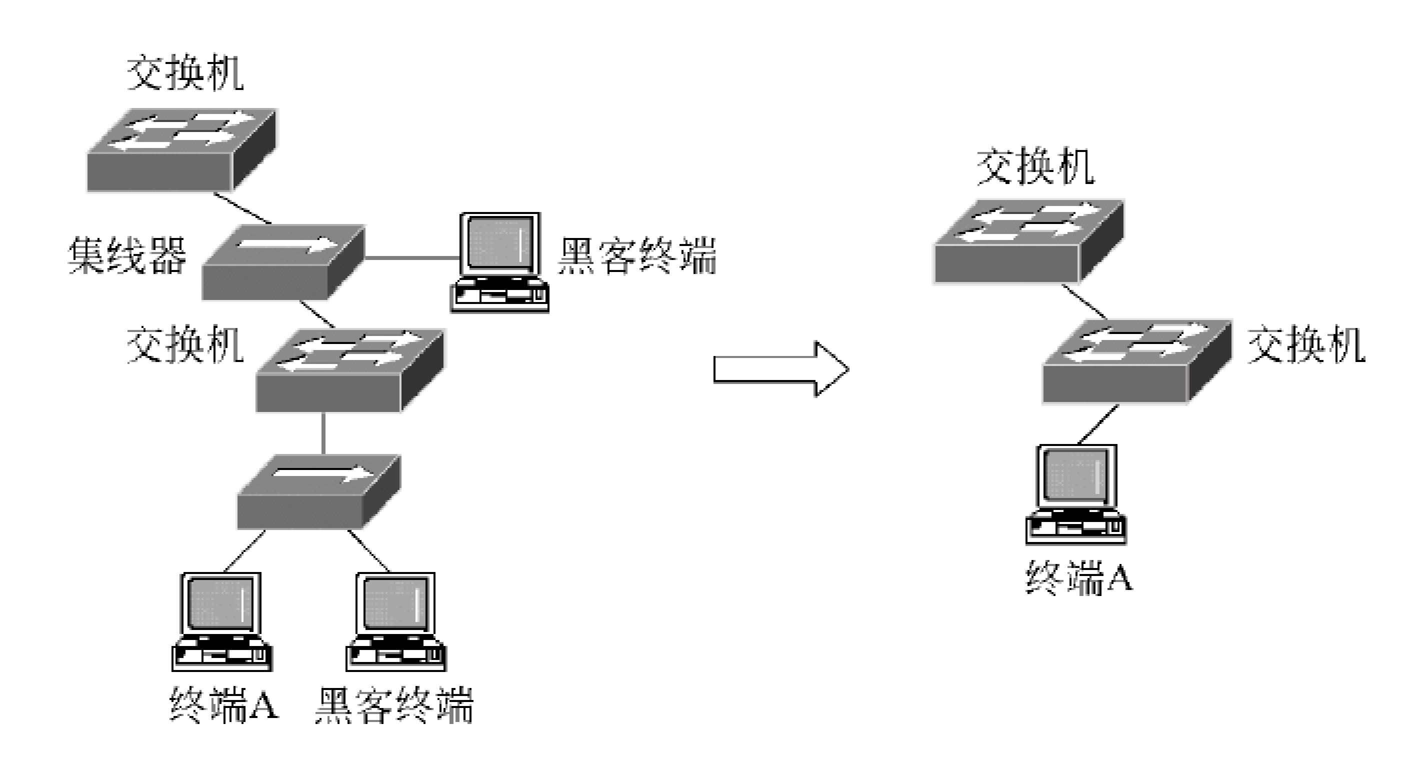


图 3.1　安全端口和全双工通信方式

5. 设备配置管理

图 3.2 中，二层交换机的设备配置管理地址属于 VLAN 1(默认 VLAN)对应的网络地址，如果三层交换机中 VLAN 1 对应的 IP 接口没有开启(down 状态)，三层交换机的路由表中没有目的网络为 VLAN 1 的路由项，其他网络中的终端就无法访问 VLAN 1，因此，只有属于 VLAN 1 的终端才能通过二层交换机的配置管理地址访问各个二层交换机并实施配置管理，这样就将二层交换机的配置管理网络与其他网络隔离，严格限制了允许管理配置二层交换机的终端。

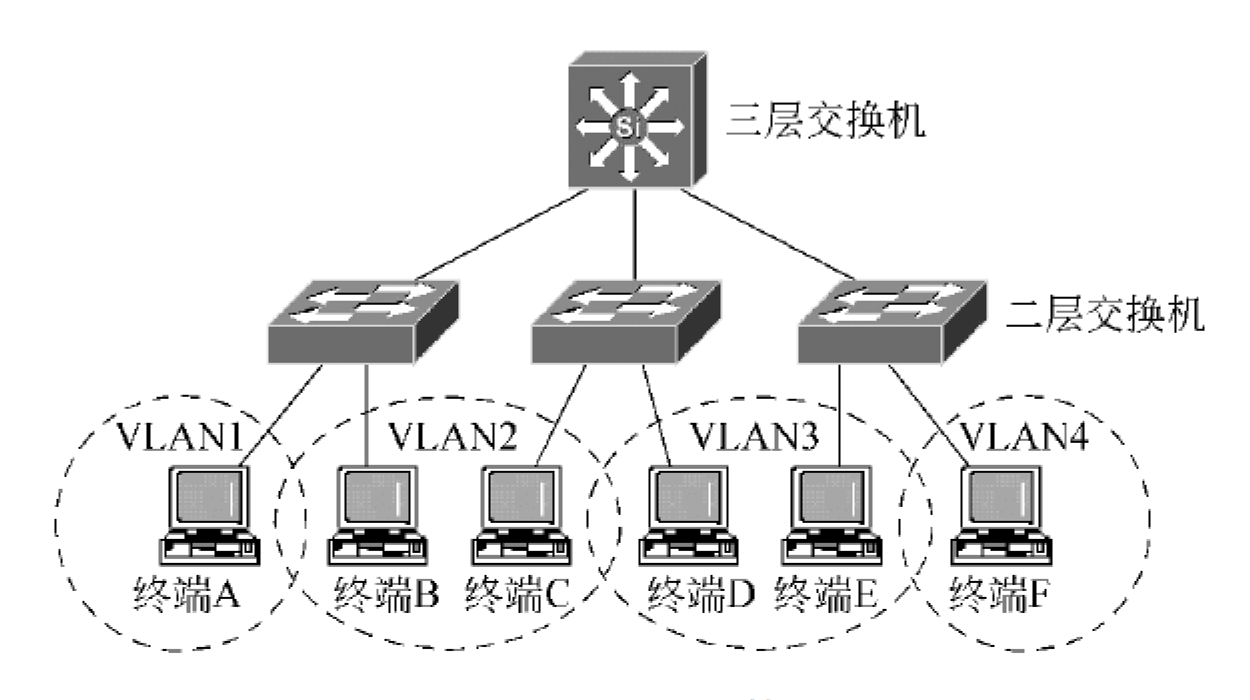


图 3.2　校园网简图

由于可以通过三层交换机的各个 IP 接口配置管理三层交换机，从网络设计上无法将三层交换机的配置管理网络和其他网络隔离，但可以通过配置管理端口的分组过滤器严格限制允许管理配置三层交换机的终端。同样可以通过配置管理端口的分组过滤器严格

限制允许管理配置二层交换机的终端。

对于图 3.3 所示的普通互连网络，可以通过任意路由器接口的 IP 地址对路由器进行配置管理。对于二层交换机，设备配置管理地址通常属于 VLAN 1(默认 VLAN)对应的网络地址。由于不存在跨路由器接口的 VLAN，因此路由器分隔的多个 VLAN 1 是独立的网络，需要分配不同的网络地址。除非每一个 VLAN 1 单独设置用于设备配置管理的终端，否则各个 VLAN 1 需要和其他网络相互通信。这种情况下，可以通过配置管理端口的分组过滤器严格限制允许管理配置二层交换机和路由器的终端。

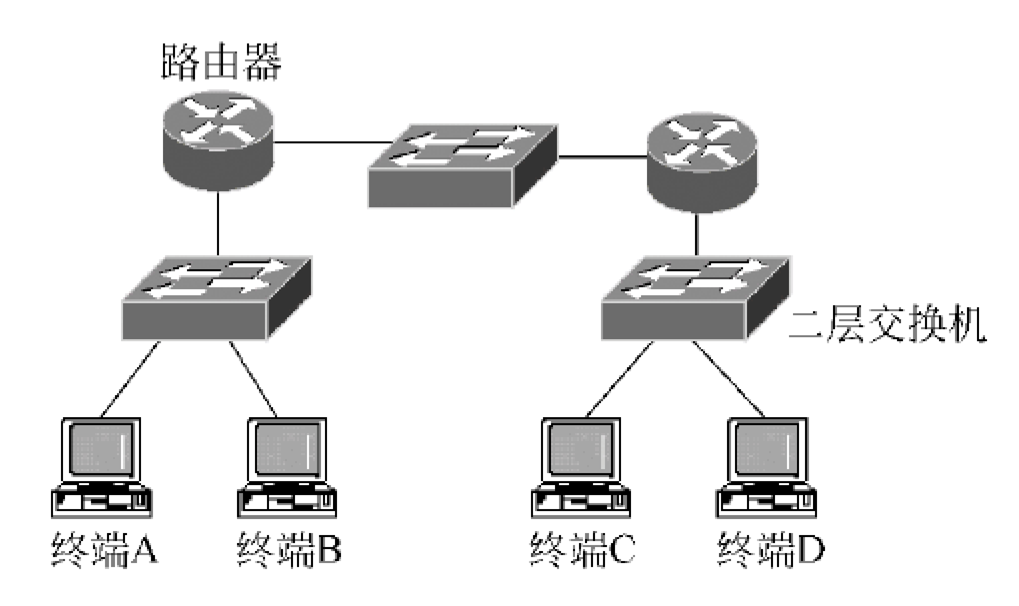


图 3.3 普通互连网络

6. 信息传输控制

简化的企业网如图 3.4 所示，分为内部网络、非军事区和外部网络三部分。为了有效抵御黑客攻击，一是通过 NAT 技术隐藏内部网络；二是通过设置访问控制策略严格控制网络之间的信息交换过程；三是通过严格控制未完成的 TCP 连接数量，防止 SYN 泛洪攻击发生。

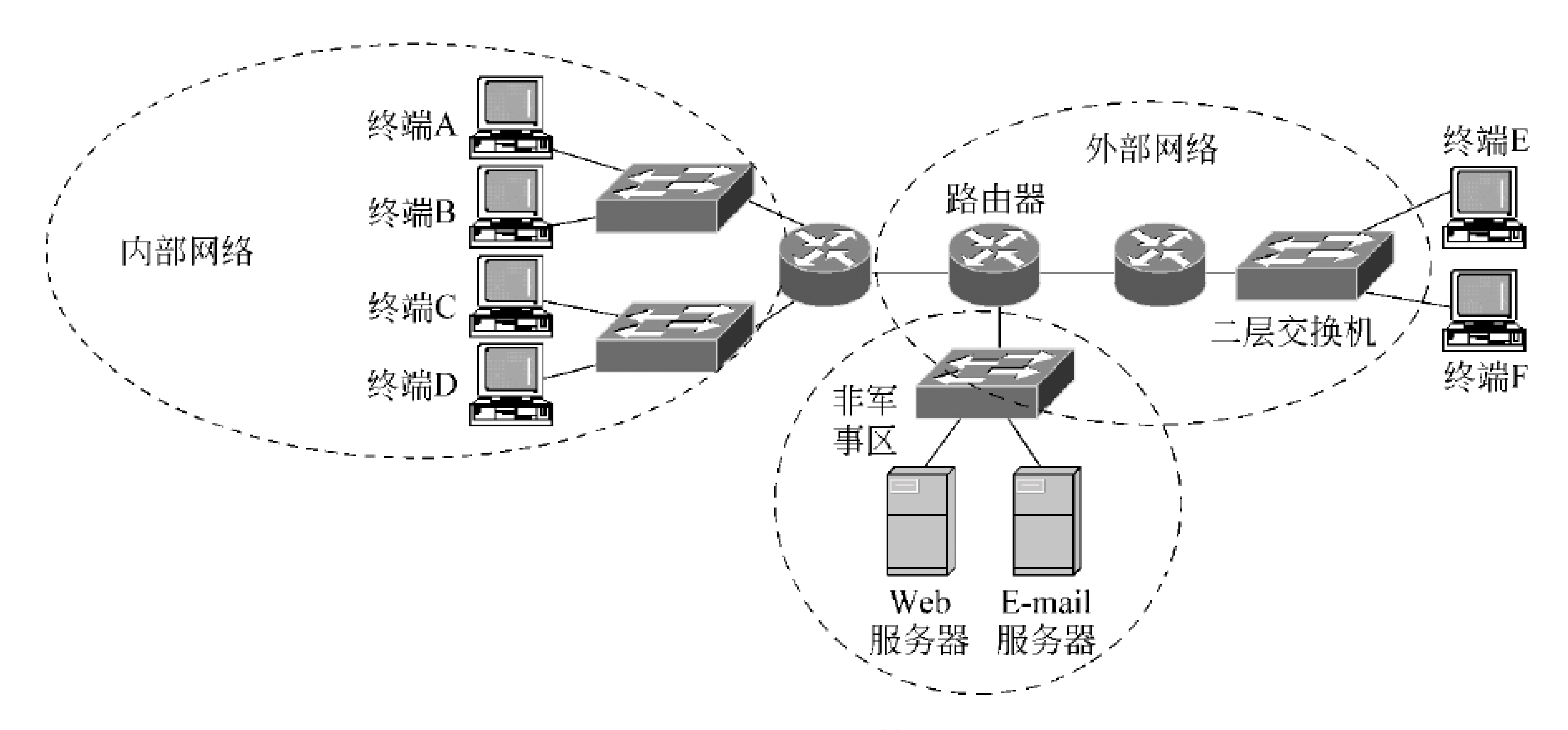


图 3.4 企业网简图

7. 流量管制

对于图 3.4 所示的企业网结构，为了防止外部网络中的黑客向内部网络传播邮件病毒，可以限制外部网络传输给非军事区中邮件服务器的 SMTP 报文的流量。

8. 安全路由

为了抵御图 3.5 所示的路由项欺骗攻击，要求对发送路由消息的路由器身份进行鉴

别，同时对接收到的路由消息的完整性进行检测，每一个路由器只处理授权路由器发送的、且传输过程中没有被篡改的路由消息。

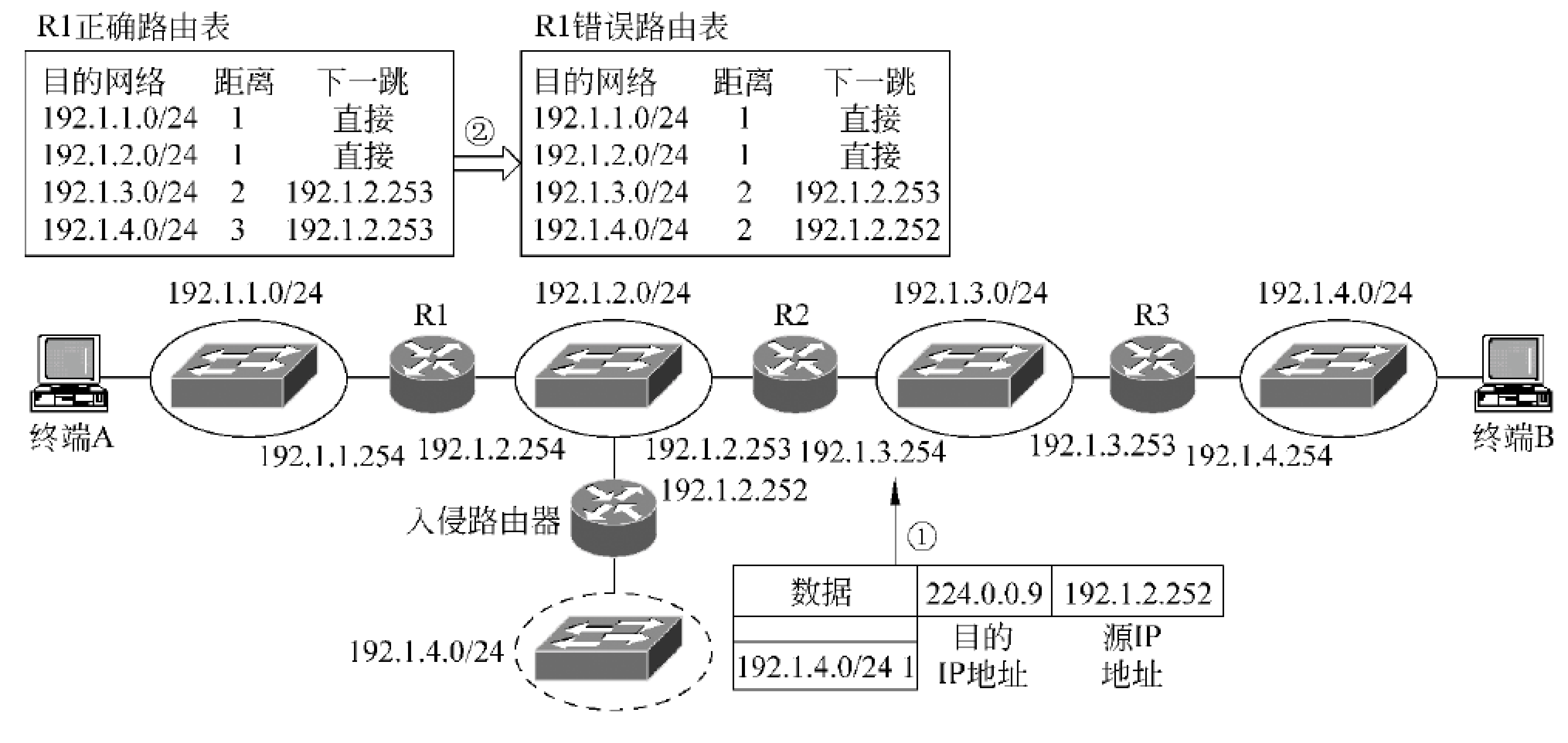


图 3.5　路由项欺骗攻击过程

9. 审计

实现审计一是建立记录网络操作过程的日志文件；二是对日志文件中的每一项记录进行分析，找出可能已经发生的网络攻击行为；三是改进网络安全策略，以应对网络面临的安全威胁。

10. DNS Sec 和应用层安全协议

如果用户得到的某个完全合格域名和 IP 地址之间的绑定关系是伪造的，用户可能被诱骗访问黑客精心设计的网站，并因此泄漏重要的私密信息。防止这种情况发生的措施有两个：一是通过 DNS Sec 对发送解析结果的 DNS 服务器的身份进行鉴别，并对接收到的解析结果进行完整性检测，防止使用黑客伪造或篡改的解析结果；二是通过应用层安全协议对访问的网站的身份进行鉴别，防止被诱骗访问黑客伪造的网站。

3.2　例题解析

3.2.1　自测题

1. 选择题

(1) 下述________不是黑客成功实施攻击的原因。

A. 主机系统漏洞　　　　B. 通信协议的安全缺陷
C. 用户警惕性不够　　　D. 网络分层结构

(2) 下述________不是黑客发现主机系统漏洞的步骤。

A. 通过主机扫描发现在线主机
B. 通过端口扫描发现开启的服务
C. 通过主动探测获得操作系统类型和版本号

D. 骗取用户口令

(3) 下述________是最主要的主机系统漏洞。

A. 缓冲器溢出 B. Unicode 漏洞 C. Ping of Death D. Land

(4) 下述________是解决主机系统漏洞的较好办法。

A. 消灭主机系统漏洞

B. 不让黑客知道已经发现的主机系统漏洞

C. 网络隔绝黑客扫描主机系统的途径

D. 将存在漏洞的主机系统和网络断开

(5) 下述________不是网络中用于隔绝黑客扫描主机系统途径的机制。

A. 接入控制 B. 网络间信息交换控制

C. 入侵防御系统的异常检测 D. 主机系统用户登录控制

(6) 下述________不是对主机系统实施的拒绝服务攻击。

A. Ping of Death B. SYN 泛洪

C. Smurf D. 穷举法猜测用户登录口令

(7) 缓冲器溢出的最大危害是________。

A. 使系统崩溃 B. 使系统运行出错

C. 管理员权限下运行黑客程序 D. 侵占其他用户内存

(8) SYN 泛洪攻击利用________。

A. 操作系统漏洞 B. 通信协议缺陷

C. 缓冲区溢出 D. 用户警惕性不够

(9) 下述________是蠕虫病毒传播的主因。

A. 缓冲区溢出漏洞

B. 从服务器下载文件

C. 收发电子邮件

D. 通过移动媒介在主机系统间复制文件

(10) 下述________不是以破坏信息保密性为目的的攻击行为。

A. 信息嗅探 B. 信息截获 C. 安装后门程序 D. DDoS

(11) 下述________不是以破坏信息完整性为目的的攻击行为。

A. 信息嗅探 B. 信息截获

C. 路由项欺骗攻击 D. ARP 欺骗攻击

(12) 下述________不是以破坏信息可用性为目的的攻击行为。

A. Ping of Death B. SYN 泛洪 C. 安装后门程序 D. DDoS

(13) 下述________攻击行为与主机系统漏洞无关。

A. Ping of Death B. Land C. 安装后门程序 D. Smurf

(14) 安装主机入侵防御系统,对下述________攻击行为作用不大。

A. 窃取信息资源 B. 篡改注册表 C. 安装后门程序 D. Smurf

(15) 安装网络入侵防御系统,对下述________攻击行为作用不大。

A. 信息嗅探 B. 利用缓冲区溢出运行黑客程序

C. 安装后门程序　　C. Smurf

(16) 防火墙实施的网络间信息交换控制，对下述________攻击行为作用不大。

A. ARP 欺骗　　B. 木马外泄信息资源

C. Ping of Death　　D. SYN 泛洪

(17) 交换机提供的安全技术，对下述________攻击行为作用不大。

A. ARP 欺骗　　B. 源 IP 地址欺骗

C. 伪造 DHCP 服务器　　D. Ping of Death

2. 填空题

(1) 主机系统漏洞是________，黑客利用某个主机系统存在的漏洞实施攻击需要完成________、________、________和________ 4 个步骤。

(2) 缓冲器溢出是最严重的主机系统漏洞，黑客可以利用缓冲器溢出________，这是蠕虫病毒快速传播的主因。

(3) ________、________、________和________属于 DoS，其中，________和________是利用主机系统漏洞实现的。

(4) ARP 欺骗、DNS 欺骗、伪造 DHCP 服务器、源 IP 地址欺骗和路由项欺骗等攻击行为中交换机安全技术能够解决的有________、________和________，路由器安全技术能够解决的有________和________。

(5) 网络中信息资源分为存储在主机系统中的信息资源和经过网络传输的信息资源两大类，________、________和________等手段非法窃取存储在主机系统中的信息资源，________、________和________等手段非法窃取经过网络传输的信息资源。

(6) 阻止黑客完成对主机系统实施攻击所需的 4 个步骤的网络安全技术有________、________和________，其中________阻止黑客终端接入网络，________阻止黑客终端向主机系统传输与实施攻击有关的信息流，________能够发现黑客正在进行的攻击行为并予以反制。

3. 名词解释

____ DoS　　____ DDoS

____伪造 DHCP 服务器　　____ DNS 欺骗

____ Smurf　　____ Ping of Death

____ SYN 泛洪　　____ Land

____ ARP 欺骗　　____源 IP 地址欺骗

____ Unicode 漏洞　　____路由项欺骗

____信息嗅探　　____信息截获

____缓冲器溢出　　____字典攻击

(a) 通过破坏，或者过度消耗主机系统和网络的资源，使得主机系统和网络无法提供正常服务的一种攻击行为。

(b) 从控制的多个主机系统同时向某个目标主机发起拒绝服务攻击的行为。

(c) 通过发送大量以网络中本不存在的 IP 地址为源地址的建立 TCP 连接请求，使得服务器 TCP 会话表被大量未完成的 TCP 连接占用，以至于无法响应正常的 TCP 连接

请求的攻击行为。

(d) 通过向目标主机发送大量以目标主机的 IP 地址为源地址的 TCP 连接请求，使得目标主机的 TCP 会话表被大量这样的 TCP 连接长期占用，以至于无法响应正常的 TCP 连接请求的攻击行为。

(e) 通过发送以目标主机 IP 地址为源地址、以某个大型网络的直接广播地址为目的地址的 ICMP ECHO 请求报文，使得大型网络中的每一个主机系统都向目标主机发送 ICMP ECHO 响应报文，并因此阻塞大型网络与目标主机之间的通路，使得目标主机无法接收发送正常报文的一种攻击行为。

(f) 一种因为分片后各段数据长度之和超过 64KB，使得接收端拼装数据时发生缓冲区溢出，并使接收端系统崩溃的攻击行为。

(g) 一种通过在 ARP 报文中给出错误的 IP 地址和 MAC 地址之间的绑定关系，使得路由器和主机系统错误地将主机系统 X 对应的 MAC 地址作为发送给主机系统 Y 的 MAC 帧的目的 MAC 地址的一种攻击行为。

(h) 一种不以发送者的 IP 地址，而以其他主机系统的 IP 地址，或者网络中不存在的 IP 地址作为 IP 分组源 IP 地址的攻击行为。

(i) 一种通过将配置错误的默认网关地址和 DNS 服务器地址的伪造的 DHCP 服务器接入网络，使得网络内的主机系统获得该伪造的 DHCP 服务器提供的错误的网络配置信息的攻击行为。

(j) 一种将错误的 IP 地址作为某个域名的解析结果的攻击行为。

(k) 一种虽然窃取经过网络传输的信息，但不影响信息传输过程的攻击行为。

(l) 一种截获经过网络传输的信息，使信息无法继续正常传输的攻击行为。

(m) 一种使得某个进程接收的信息超出分配给该进程的缓冲器容量，并使超出部分的信息覆盖分配给其他进程的缓冲器空间的攻击行为。

(n) 一种将一切可能成为口令的字符串集合作为字典文件，并用程序自动地逐个尝试字典文件中的字符串登录目标主机的攻击行为。

(o) 一种直接用 Unicode 输入禁止输入的字符串模式的攻击行为。

(p) 一种通过发送错误的路由消息或链路状态信息，使得路由器生成错误的通往某个目的网络的传输路径的攻击行为。

4. 判断题

(1) 操作系统和应用程序漏洞是可以消除的。

(2) 针对主机系统漏洞实施的攻击是无法防御的。

(3) 在被攻击前，通过补丁软件消除某个已经发现的漏洞是一种有效的抵御攻击的手段。

(4) 在无数漏洞中，缓冲器溢出漏洞是危害较大的一种漏洞。

(5) 缓冲器溢出漏洞是蠕虫得以快速传播的主因。

(6) Smurf 这样的拒绝服务攻击是无法防御的。

(7) 黑客攻击过程和正常访问过程是有所区别的，只是这种区别不是黑白那样分明。

(8) 网络设备本身也是黑客的攻击目标，需要重点保护。

(9) 黑客实施攻击需要具备多项条件,网络安全技术可以阻止这些条件成立。

(10) 只要目的 IP 地址正确,IP 分组能够到达目的终端。

(11) 单一网络安全技术的作用有限。

3.2.2 自测题答案

1. 选择题答案

(1) D,分层是复杂系统的有效设计方法,能够提高系统的可靠性和安全性。

(2) D,这一项和主机系统漏洞无关。

(3) A,黑客利用缓冲器溢出漏洞能够实现在管理员权限下运行自编程序,这一点对主机系统的危害极大。

(4) C,其他三项中,A 和 B 项做不到,D 项是笨办法。

(5) D,登录的前提是已经建立黑客和主机系统之间的传输通路。

(6) D,拒绝服务攻击是使主机系统丧失服务能力,D 项不会使主机系统崩溃。

(7) C,管理员权限下运行黑客程序,可以任意处理系统资源。

(8) B,TCP 连接建立过程存在缺陷。

(9) A,黑客利用缓冲器溢出漏洞实现在管理员权限下运行自编程序是蠕虫能够自动传播并激活的基础。

(10) D,拒绝服务攻击一般以破坏可用性为目的。

(11) A,破坏信息完整性首先需要截获信息,然后篡改信息。

(12) C,后门程序为了隐蔽,一般不会影响主机系统正常服务功能。

(13) D,这种拒绝服务攻击是任何主机系统自身无法抵御的。

(14) D,加强主机系统自身功能对抵御这种拒绝服务攻击是徒劳的。

(15) A,网络入侵防御系统需要发现异常信息流,然后才能对异常信息流实施干预,信息嗅探攻击不会导致信息流异常。

(16) A,ARP 欺骗攻击在网络内部进行,无需经过防火墙。

(17) D,这项攻击需要拼装完分片后产生的所有数据片才能发现,交换机一般不具有这项功能。

2. 填空题答案

(1) 无法消除的,信息收集,扫描,渗透,攻击。

(2) 在管理员权限下运行自编程序。

(3) Ping of Death,SYN 泛洪,Land,Smurf,Ping of Death,Land。

(4) ARP 欺骗,伪造 DHCP 服务器,源 IP 地址欺骗,源 IP 地址欺骗,路由项欺骗。

(5) 木马,非法登录主机系统,利用缓冲器溢出漏洞在管理员权限下运行黑客程序,ARP 欺骗,路由项欺骗,交换机间插入集线器嗅探信息。

(6) 交换机接入控制技术,防火墙,网络入侵防御系统,交换机接入控制技术,防火墙,网络入侵防御系统。

3. 名词解释答案

a DoS	b DDoS
i 伪造 DHCP 服务器	j DNS 欺骗
e Smurf	f Ping of Death
c SYN 泛洪	d Land
g ARP 欺骗	h 源 IP 地址欺骗
o Unicode 漏洞	p 路由项欺骗
k 信息嗅探	l 信息截获
m 缓冲器溢出	n 字典攻击

4. 判断题答案

(1) 错,目前软件设计方法下,消除漏洞是无法实现的。

(2) 错,黑客攻击某个主机系统首先需要建立与该主机系统之间的传输通路,然后发现该主机系统存在的漏洞,并针对该漏洞实施攻击,网络安全技术可以阻止黑客完成上述的每一个步骤。

(3) 对,这样可以防止黑客针对该漏洞实施的攻击。

(4) 对,黑客能够利用缓冲器溢出漏洞在管理员权限下运行自编程序。

(5) 对,利用缓冲器溢出漏洞在管理员权限下运行自编程序是蠕虫自动传播和激活的技术基础。

(6) 错,交换机和路由器防御源 IP 地址欺骗攻击的安全技术与最后一跳路由器过滤掉以直接广播地址为目的地址的 IP 分组的过滤技术都是有效防御手段。

(7) 对,这是网络入侵防御系统既是防御黑客攻击的有效手段,但又不能完全消除黑客攻击的原因。

(8) 对,被黑客控制网络设备的后果是无法想象的。

(9) 对,网络安全技术对防御黑客攻击是有所作为的。

(10) 错,有太多的原因不能使目的地址正确的 IP 分组到达正确的目的终端。

(11) 对,每一种网络安全技术有着适用范围和局限。

3.2.3 简答题解析

1. 黑客能够成功入侵主机系统的原因及应对策略。

回答: 原因在于:一是基于当前的软件设计理论和方法,从根本上消除大型软件(操作系统和大型的应用程序)的漏洞是不可能的;二是随着时间的推移,使用的用户增多,漏洞终将被发现,还有一些组织和机构专门研究流行操作系统和应用程序的漏洞,并公开研究结果;三是一旦发现漏洞,就会出现针对该漏洞的攻击软件,并流行开来;四是只要某个主机系统还没有用补丁软件修补该漏洞,黑客就可通过针对该漏洞的攻击软件对该主机系统实施攻击。

应对策略分为以下三个方面:

一是黑客成功攻击某个主机系统的步骤包括:①建立与该主机系统之间的传输通路。②通过扫描发现该主机系统的操作系统或应用程序存在漏洞且没有用补丁软件修

补。③使用针对该漏洞的攻击软件实施攻击。网络安全技术可以阻止黑客完成这些步骤，比如通过接入控制阻止黑客终端接入网络，通过防火墙的访问控制策略阻止黑客终端向该主机系统传输与漏洞扫描和攻击有关的报文，通过网络入侵防御系统发现黑客正在实施的扫描和攻击行为，并予以反制。

二是主机入侵防御系统能够对主机资源的访问过程实施严格管制，黑客攻击主机系统的目的或是窃取主机系统信息资源；或是破坏主机系统资源，使其崩溃；或是建立后门，以便长期控制该主机系统，完成这些操作都需黑客完成对主机系统核心资源的访问，如果主机入侵防御系统能够有效阻止黑客完成对主机系统核心资源的访问，黑客将无法继续对该主机系统的攻击行为。

三是及时下载并运行补丁软件，只要在黑客针对该漏洞对主机系统实施攻击前，主机系统通过补丁软件修补了该漏洞，黑客针对该漏洞对主机系统实施的攻击将无法成功。

2. 简述拒绝服务攻击的应对措施。

回答：拒绝服务攻击可以分为针对主机系统漏洞实施的拒绝服务攻击和以过度消耗主机系统资源，使其无法正常与其他主机系统通信并提供服务的拒绝服务攻击两种。对于前一种，如 Ping of Death、Land，一是可以通过修正操作系统和协议实现程序的漏洞予以解决；二是实施这种类型拒绝服务攻击的报文具有一定特征，网络中的信息传输设备和信息交换控制设备，如路由器、防火墙和网络入侵防御系统能够检测出具有该类特征的报文，并予以丢弃。对于后一种拒绝服务攻击，如 Smurf，一是攻击报文通常采用原本不存在的 IP 地址，或攻击目标的 IP 地址作为源 IP 地址；二是攻击过程中某种类型的流量会出现异常。因此可以采用以下应对措施：一是可以通过交换机的接入控制过程和路由器的单播反向路径验证功能禁止源 IP 地址不正确的 IP 分组进入网络；二是通过分布式网络入侵防御系统对各种类型报文的流量进行监控，一旦出现较大范围的波动，立即示警，并予以反制；三是可以通过流量管制器对一些和常见拒绝服务攻击有关的报文类型的流量进行管制。

3. 简述利用缓冲器溢出漏洞运行黑客程序的原理。

回答：缓冲区溢出过程如图 3.6 所示，图左边是正常的缓冲区分配结构，由于函数 B 使用缓冲区时没有检测缓冲区边界这一步，当函数 B 的输入数据超过规定长度时，函数 B 的缓冲区发生溢出，超过规定长度部分的数据将继续占用其他存储空间，覆盖用于保留函数 A 的返回地址的存储单元。如果黑客终端知道主机系统某个功能块中存在缓冲区溢出漏洞，即该功能块使用缓冲区时不检测缓冲区边界，黑客可以精心设计发送给该功能块处理的数据，如图 3.6 右边所示。黑客发送给该功能块的数据中包含某段恶意代码，而且用于覆盖函数 A 返回地址的数据恰恰是该段恶意代码的入口地址，这样当系统返回到函数 A 时，实际上是开始运行黑客上传的恶意代码。如果函数 A 具有管理员权限，则在管理员权限下运行黑客上传的恶意代码，黑客上传的恶意代码可以完成对主机系统核心资源的访问，例如，创建具有管理员权限的用户；从黑客创建的文件服务器下载动态链接库，并将其集成到主机系统的动态链接库中等。这些操作对主机系统的危害极大且影响长远。

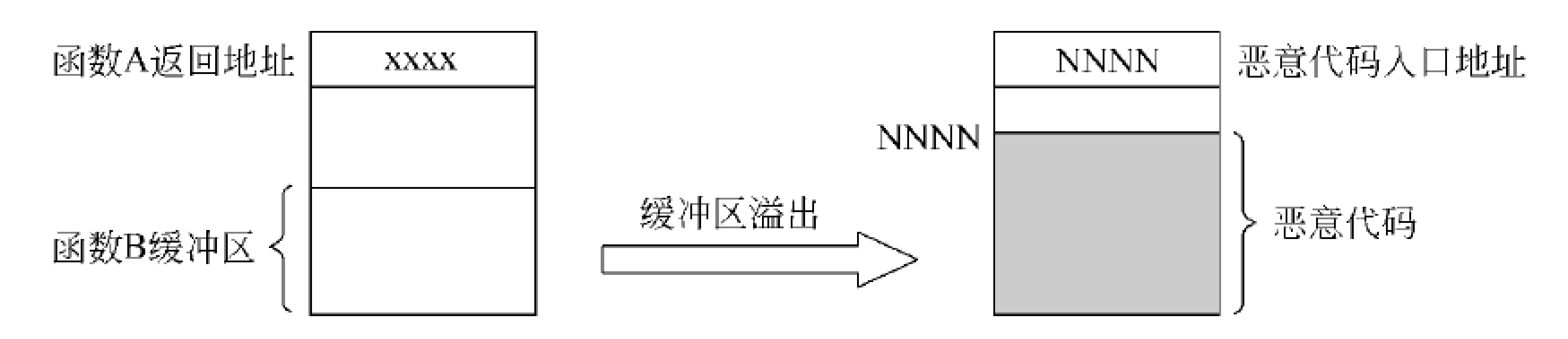


图 3.6 缓冲区溢出过程

3.2.4 综合题解析

设计一个企业网，使其具有以下用于防御黑客攻击的功能。

- 只允许特定终端对网络设备进行远程配置；
- 限制接入内部网络的终端；
- 网络中不允许出现方便信息嗅探的广播信道；
- 通过访问控制策略阻止可能和黑客攻击有关的信息交换过程进行；
- 通过安全路由技术保证路由器建立正确的路由表；
- 通过对特定类型的信息流实施流量管制，防止黑客进行拒绝服务攻击；
- 要求日志服务器记录发生在网络设备上的事件，以便通过审计发现黑客的攻击行为。

解析：企业网网络结构如图 3.7 所示。为了实施访问控制策略，将企业网分为内部网络、非军事区和外部网络三部分，内部网络本身可以分为安全等级不同的若干子网。

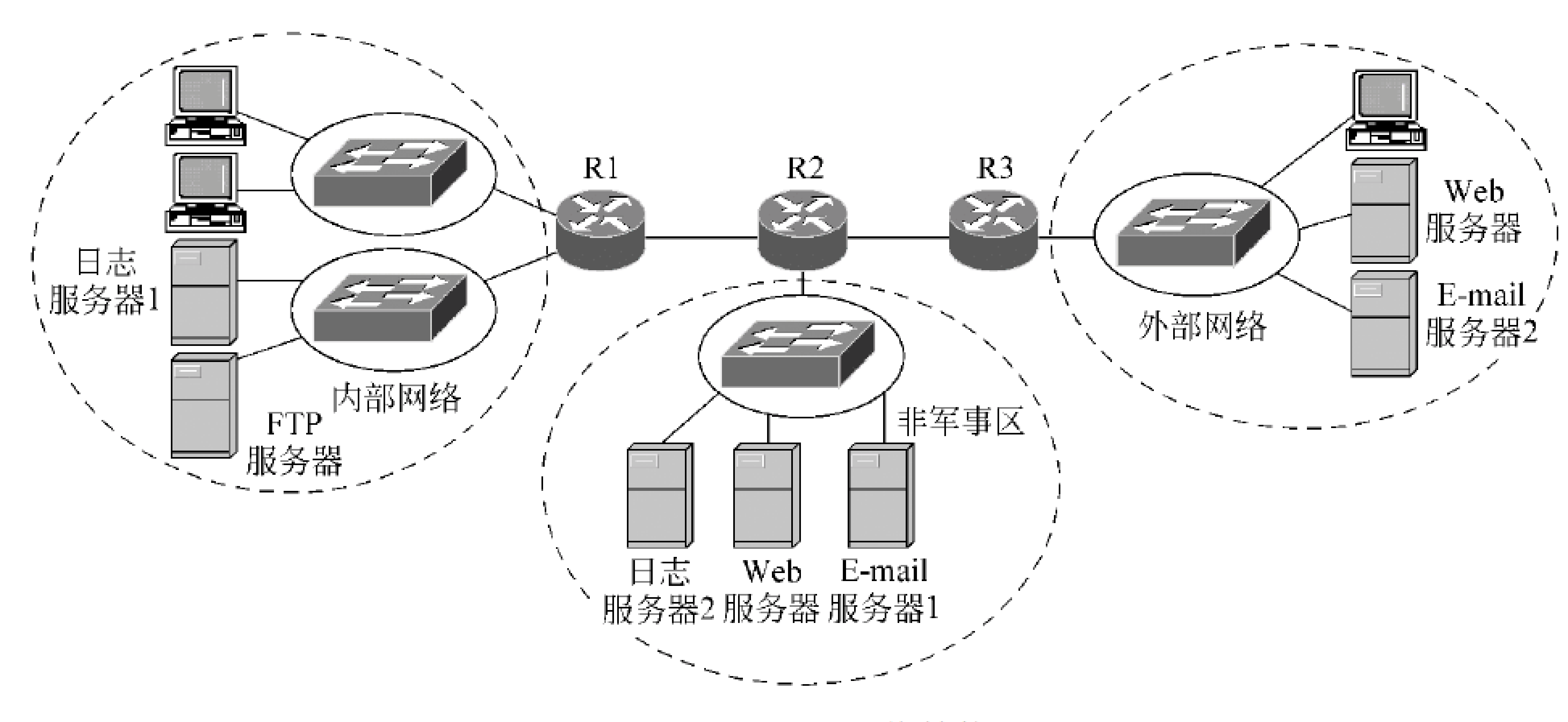


图 3.7 企业网网络结构

(1) 企业网中的所有网络设备允许远程配置，但一是通过设置口令只允许授权用户配置网络设备；二是通过对网络设备中的虚拟终端加载访问控制列表，只允许特定 IP 地址的终端和该网络设备中的虚拟终端通信。

(2) 可以通过将每一个交换机端口和 MAC 地址，或者 IP 地址和 MAC 地址对静态绑定，只允许特定 MAC 地址，或者特定 MAC 地址和 IP 地址的终端接入该交换机端口。也可以通过 802.1X 基于用户对用户终端接入交换机端口过程实施控制。

(3) 所有以太网端口静态配置成全双工通信方式，不允许广播信道(如集线器)接入任何交换机端口，避免黑客通过广播信道嗅探信息。

(4) 设置如下访问控制策略。

① 只允许内部网络终端访问内部网络服务器；

② 允许内部网络终端发起访问非军事区中的服务器和外部网络中的 Web 服务器；

③ 允许内部网络终端通过 ICMP 报文对非军事区中的服务器进行管理；

④ 允许内部网络终端通过 Telnet 或 SSH 访问路由器 R2、R3 和非军事区中的二层交换机；

⑤ 允许非军事区中的 E-mail 服务器和外部网络中的 E-mail 服务器相互交换 SMTP 报文；

⑥ 允许外部网络中的终端访问非军事区中的 Web 服务器；

⑦ 禁止其他信息交换过程。

通过设置上述访问控制策略，使得外部网络中的终端无法直接对内部网络发起攻击，通过限制外部网络终端和非军事区中服务器之间相互交换的报文类型，抑制外部网络终端对非军事区中服务器发起的攻击。

(5) 对路由器 R2 和 R3 检测到的未完成的 TCP 连接数设置上限，一旦路由器记录的未完成 TCP 连接数达到设置的上限，路由器通过向 TCP 连接的两端发送 RST 报文来释放未完成的 TCP 连接，直到未完成的 TCP 连接数到达设置的下限，以此抑制 SYN 泛洪攻击。

(6) 要求路由器发送的 Hello 报文和链路状态信息携带鉴别信息和序号，只接收和处理通过源端鉴别、完整性检测且确定不是重放的 Hello 报文和链路状态信息，以此抑制路由项欺骗攻击。

(7) 对内部网络终端发送给非军事区中的 ICMP 报文的流量，对外部网络终端发送给非军事区中的 SMTP 报文的流量进行管制，阻止内部网络感染病毒的终端发起对非军事区中的服务器的拒绝服务攻击和外部网络终端向内部网络终端传播邮件病毒。

(8) 在日志服务器中记录每一次对设备进行的登录和配置操作，以便通过审计发现黑客对网络设备发起的攻击。在日志服务器 1 中记录对内部网络设备和路由器 R1 进行的操作，在日志服务器 2 中记录对非军事区中设备和路由器 R2、R3 进行的操作。

3.3 实　　验

3.3.1 交换式以太网远程设备配置实验

1. 实验内容

(1) 划分 VLAN。

(2) 隔离默认 VLAN。

(3) 配置二层交换机管理地址。

(4) 验证远程配置过程。

2. 网络结构

交换式以太网结构如图 3.8 所示。S1、S2 和 S3 为二层交换机,S4 为三层交换机,一旦对 S4 配置 IP 接口,则可以通过任何一个 IP 接口的地址对 S4 实现远程配置,对二层交换机必须配置管理地址,这里,管理地址属于默认 VLAN(VLAN 1,图中用 V1 表示)对应的网络地址。针对图 3.8 所示的交换式以太网,要求默认 VLAN 与其他 VLAN 隔离,即属于默认 VLAN 的终端无法与属于其他 VLAN 中的终端通信,意味着只有属于 VLAN 1 的终端才能远程配置二层交换机。只允许属于 VLAN 2(图中用 V2 表示)的终端远程配置 S4。图中 VLAN 1~VLAN 4 对应的网络地址分别为 192.1.1.0/24、192.1.2.0/24、192.1.3.0/24 和 192.1.4.0/24。S1~S3 配置的管理地址为 192.1.1.11~192.1.1.13。

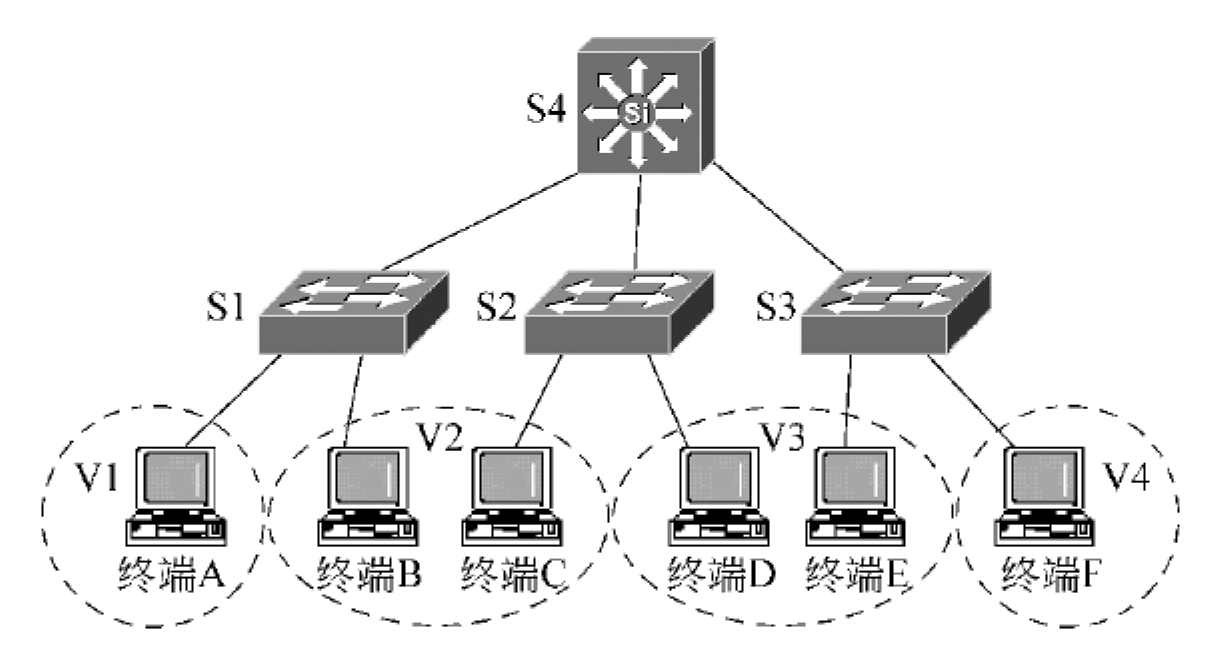


图 3.8 交换式以太网结构

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 3.8 所示的网络结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图 3.9 所示。

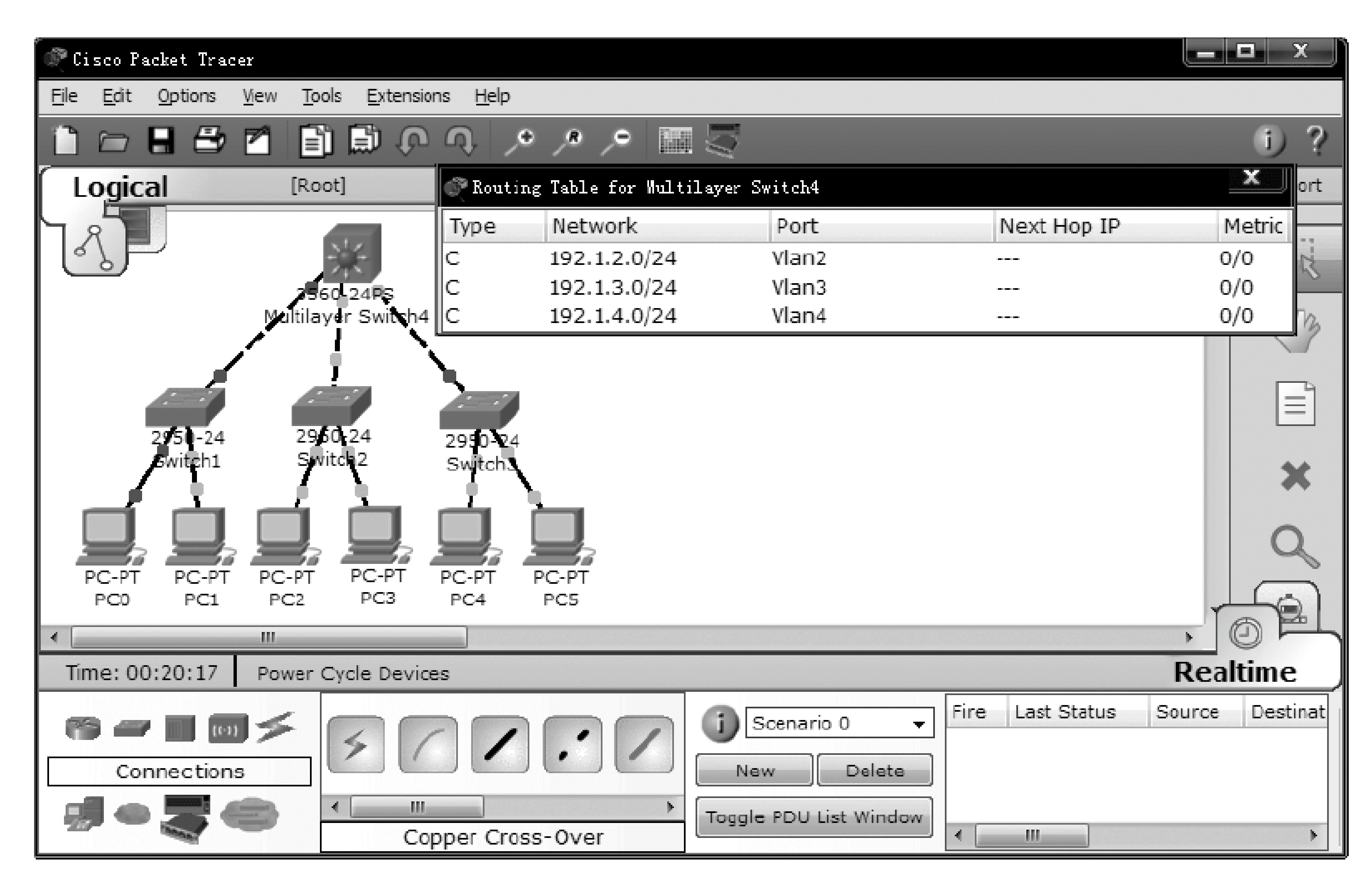


图 3.9 放置和连接设备后的逻辑工作区界面及路由表

(2) 在 Switch1 中定义 VLAN 2,将端口 FastEthernet0/2 作为非标记端口(Access 端口)分配给 VLAN 2,将端口 FastEthernet0/3 定义为被 VLAN 1 和 VLAN 2 共享的标记端口(Trunk 端口)。在 Switch2 中定义 VLAN 2 和 VLAN 3,将端口 FastEthernet0/1 作为非标记端口分配给 VLAN 2,将端口 FastEthernet0/2 作为非标记端口分配给 VLAN 3,将端口 FastEthernet0/3 定义为被 VLAN 1、VLAN 2 和 VLAN 3 共享的标记端口。在 Switch3 中定义 VLAN 3 和 VLAN 4,将端口 FastEthernet0/1 作为非标记端口分配给 VLAN 3,将端口 FastEthernet0/2 作为非标记端口分配给 VLAN 4,将端口 FastEthernet0/3 定义为被 VLAN 1、VLAN 3 和 VLAN 4 共享的标记端口。图 3.10 给出 Switch1 定义 VLAN 2 的界面,图 3.11 给出将端口 FastEthernet0/1 作为非标记端口

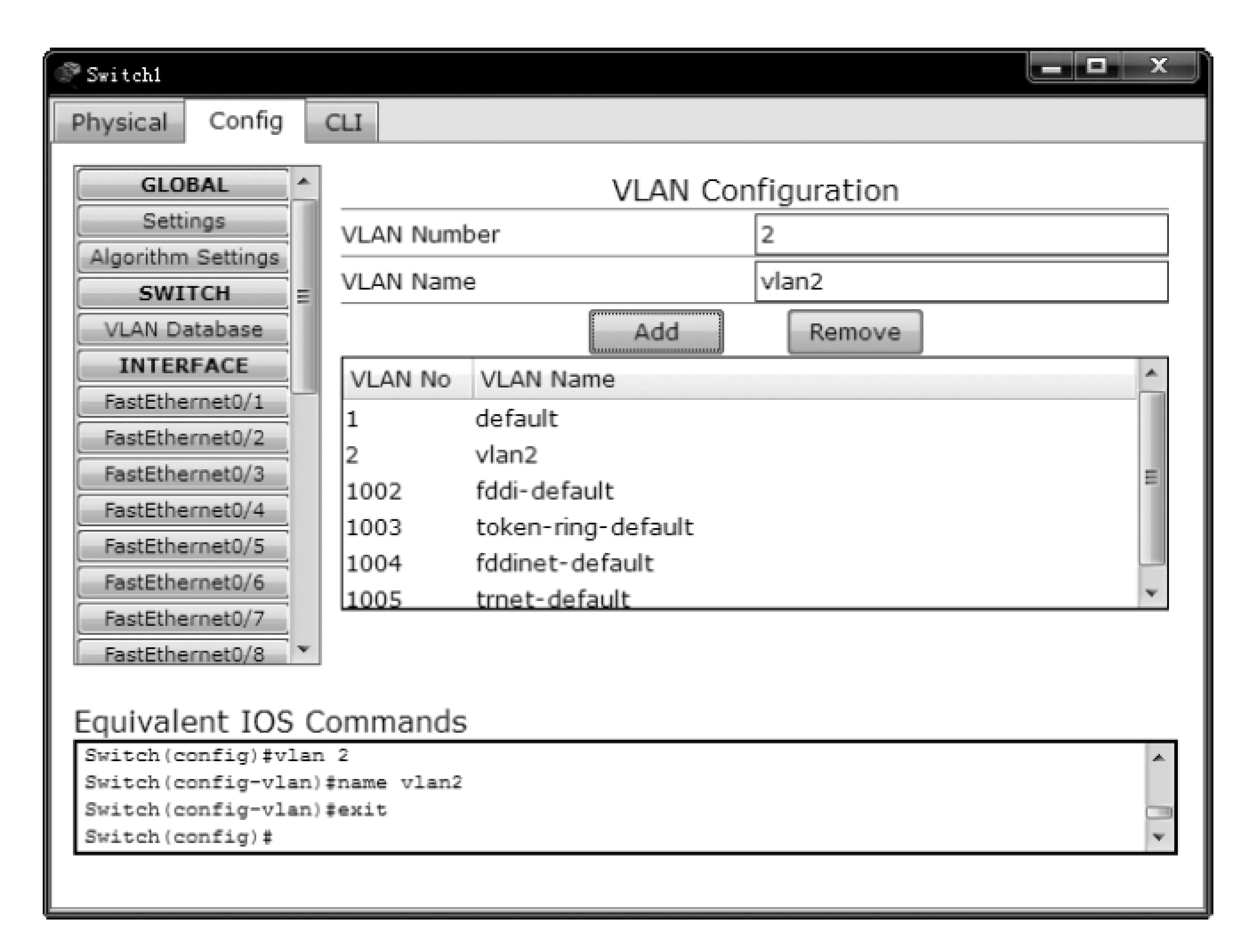


图 3.10　创建 VLAN 界面

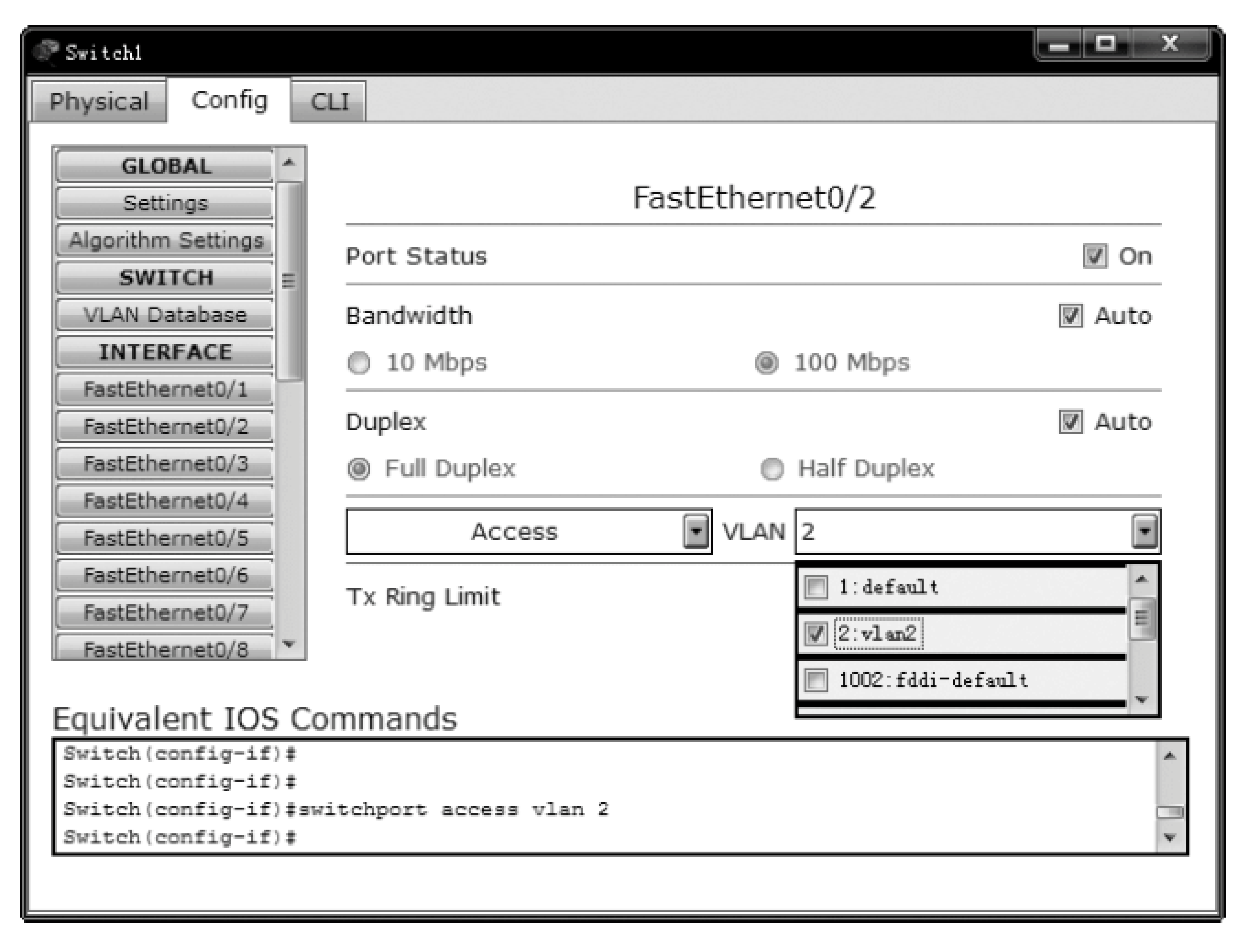


图 3.11　配置非标记端口界面

分配给 VLAN 2 的界面,图 3.12 给出将端口 FastEthernet0/3 定义为标记端口的界面,一旦某个端口被定义为标记端口,除非用命令指定共享该端口的 VLAN 范围,该端口被交换机中所有已经定义的 VLAN 所共享。



图 3.12 配置标记端口界面

(3) 在 Switch4 中定义 VLAN 2、3 和 4,端口 FastEthernet0/1 被 VLAN 1 和 2 共享,端口 FastEthernet0/2 被 VLAN 1、2 和 3 共享,端口 FastEthernet0/3 被 VLAN 1、3 和 4 共享。分别定义对应 VLAN 2、3 和 4 的 IP 接口,为 IP 接口分配 IP 地址 192.1.2.254、192.1.3.254 和 192.1.4.254。完成 IP 接口定义和 IP 地址分配后,Switch4 建立图 3.9 所示的路由表。需要指出的是,路由表中没有 VLAN 1 对应的路由项,因此 VLAN 1 对其他 VLAN 中的终端是透明的。

(4) 通过命令为 Switch1、Switch2 和 Switch3 配置管理地址,二层交换机的管理地址是默认 VLAN——VLAN 1 对应的 IP 接口地址,属于为 VLAN 1 配置的网络地址 192.1.1.0/24,这里分别是 192.1.1.11、192.1.1.12 和 192.1.1.13,需要通过命令 no shutdown 开启 VLAN 1 对应的 IP 接口。

(5) 为了实现远程配置,在二层和三层交换机的虚拟终端接口配置口令。由于二层交换机的设备管理地址属于 VLAN 1 对应的网络地址,而 VLAN 1 又和其他 VLAN 隔离,因此只能由连接在 VLAN 1 上的终端通过 Telnet 远程配置二层交换机。由于可以通过任何 IP 接口地址访问三层交换机,因此需要通过设置访问控制列表限定授权远程配置三层交换机的终端范围,这里只允许属于网络 192.1.2.0/24 的终端通过 Telnet 远程配置三层交换机。

(6) 连接在 VLAN 1 上的 PC0 配置和网络地址 192.1.1.0/24 一致的网络信息,如图 3.13 所示。PC0 远程配置二层交换机的界面如图 3.16 所示。连接在 VLAN 2 上的 PC1 配置和网络地址 192.1.2.0/24 一致的网络信息,如图 3.14 所示。由于 VLAN 1 和

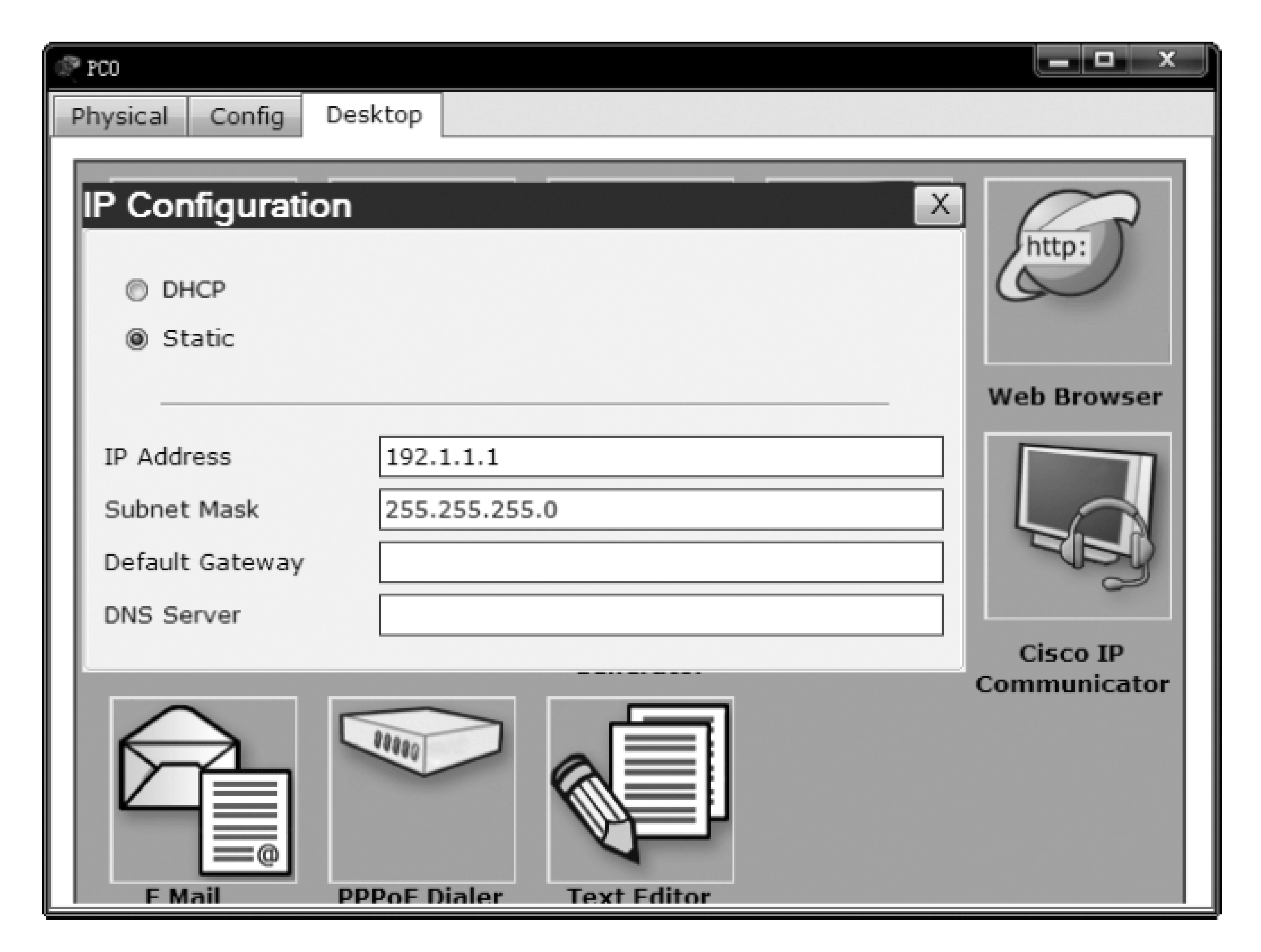


图 3.13　为属于 VLAN 1 的 PC0 配置网络信息界面

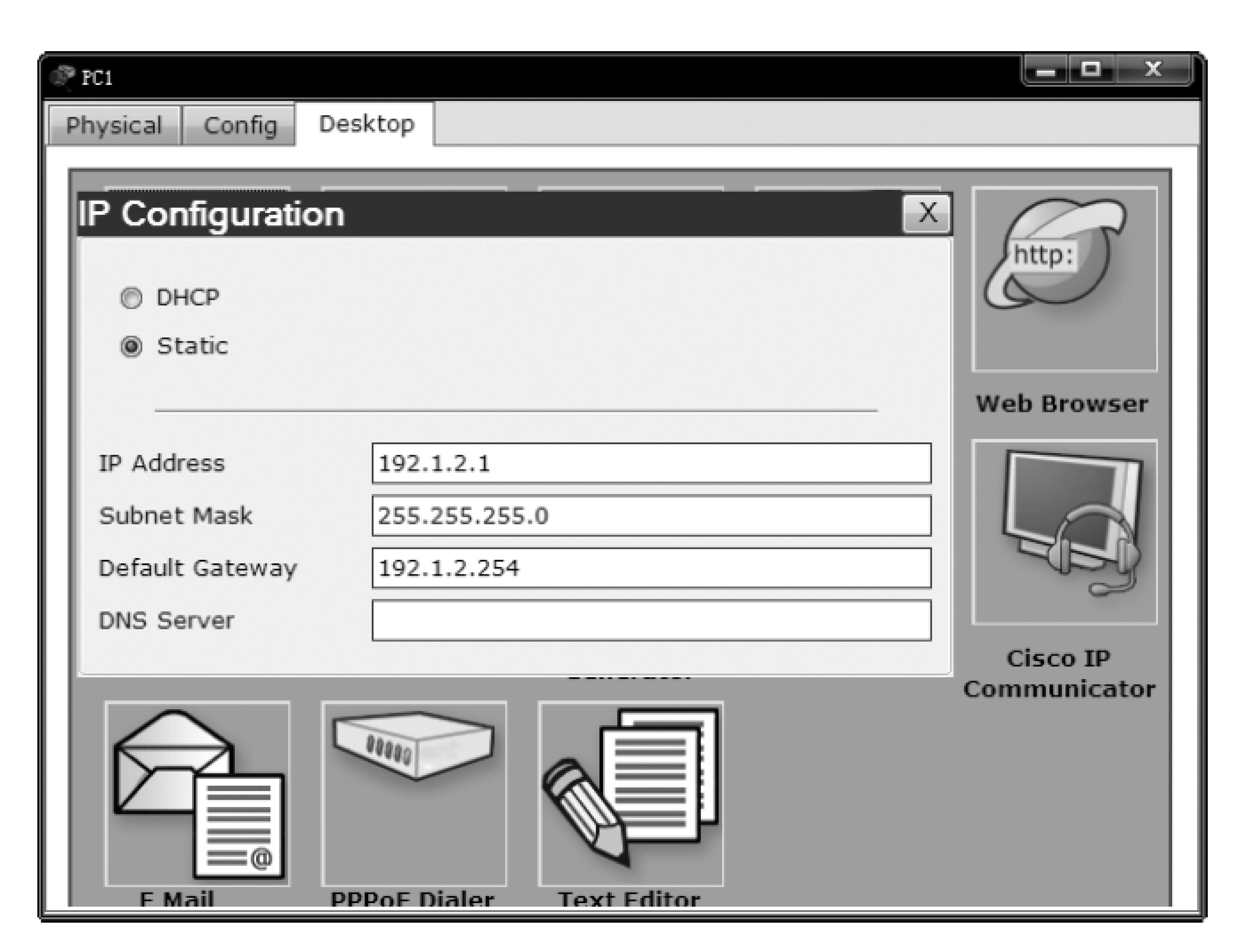


图 3.14　为属于 VLAN 2 的 PC2 配置网络信息界面

其他 VLAN 隔离，因此 PC1 无法远程配置二层交换机，但可以远程配置三层交换机，PC1 远程配置三层交换机的界面如图 3.17 所示。连接在 VLAN 3 上的 PC3 配置和网络地址 192.1.3.0/24 一致的网络信息，如图 3.15 所示。虽然 PC3 可以访问到三层交换机的 IP 接口地址，但由于三层交换机通过配置访问控制列表只允许属于网络 192.1.2.0/24 的终端远程配置它，因此 PC3 无法远程配置二层交换机和三层交换机，PC3 远程配置三层交换机失败的界面如图 3.18 所示。

4. 命令行配置过程

（1）Switch3 命令行配置过程。

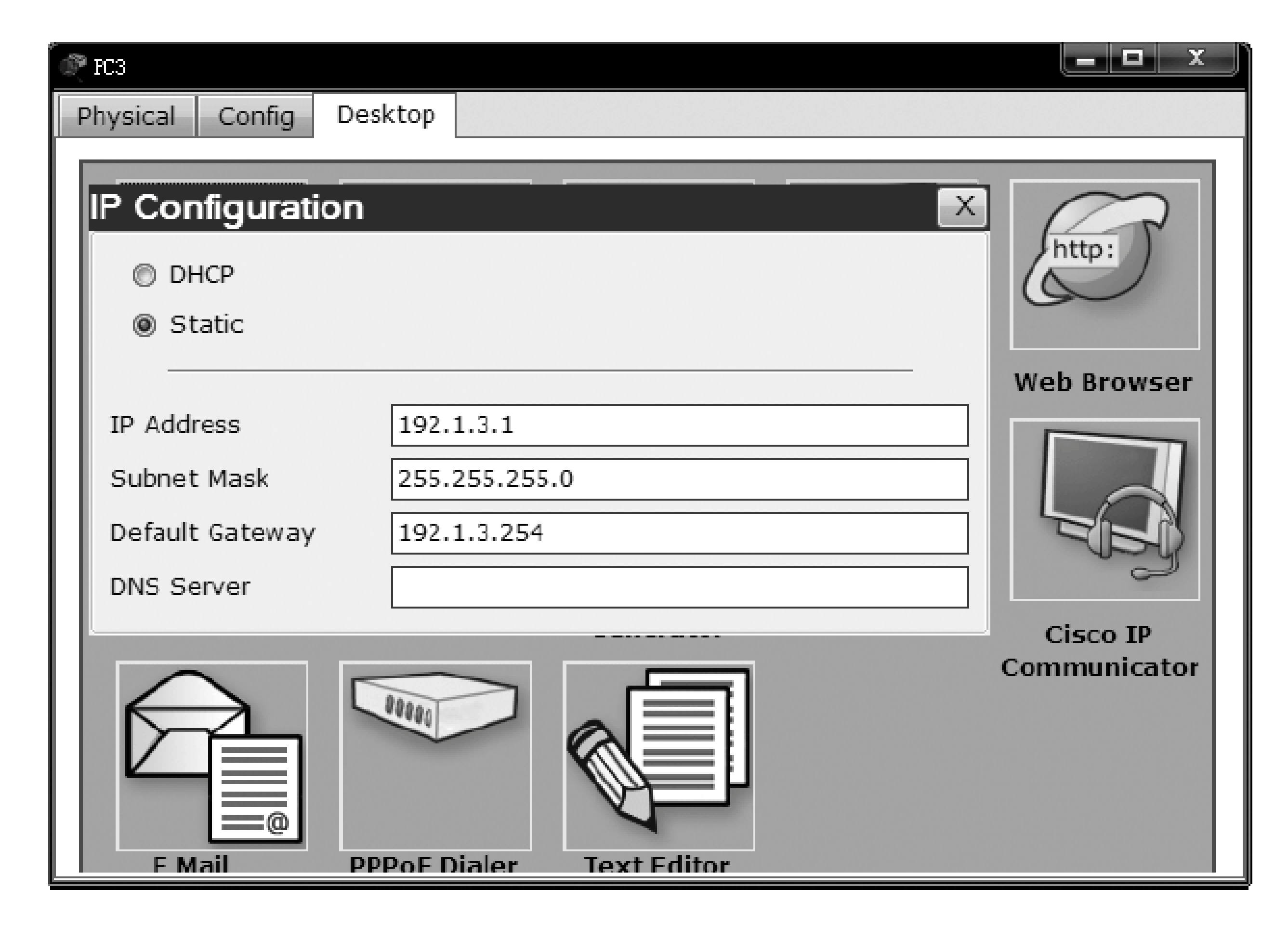


图 3.15 为属于 VLAN 3 的 PC3 配置网络信息界面

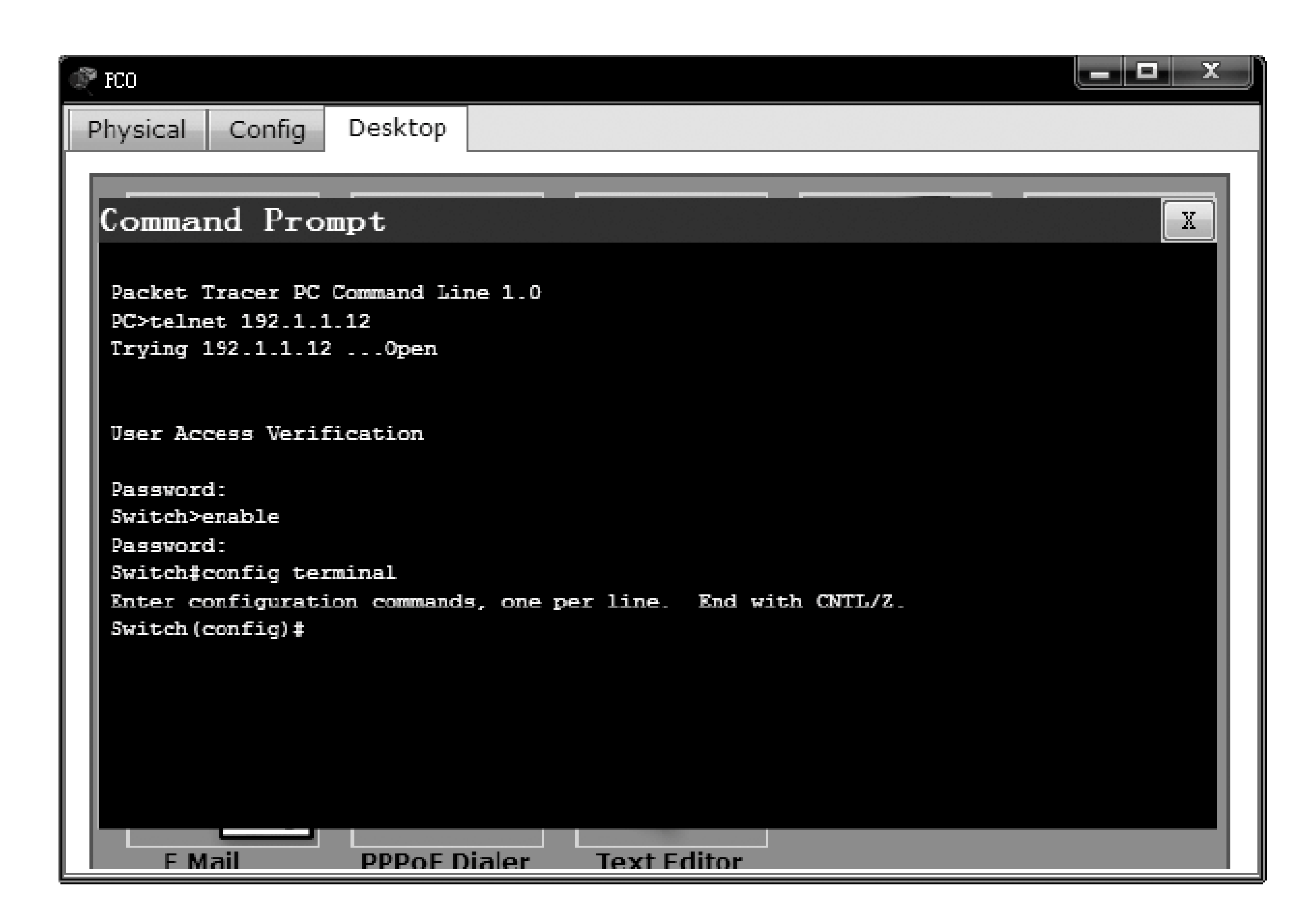


图 3.16 PC0 远程配置 Switch2 界面

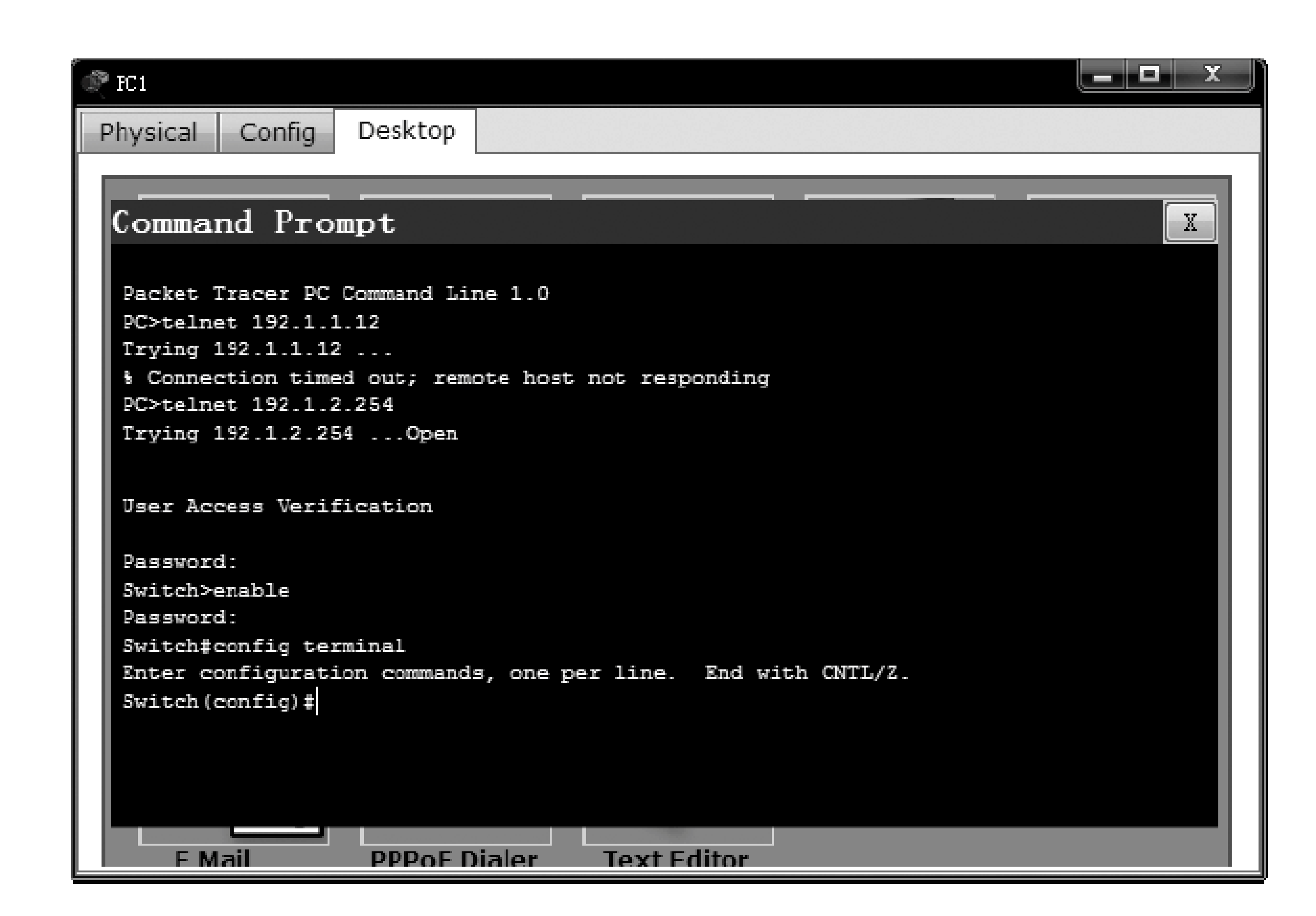


图 3.17 PC1 远程配置三层交换机界面

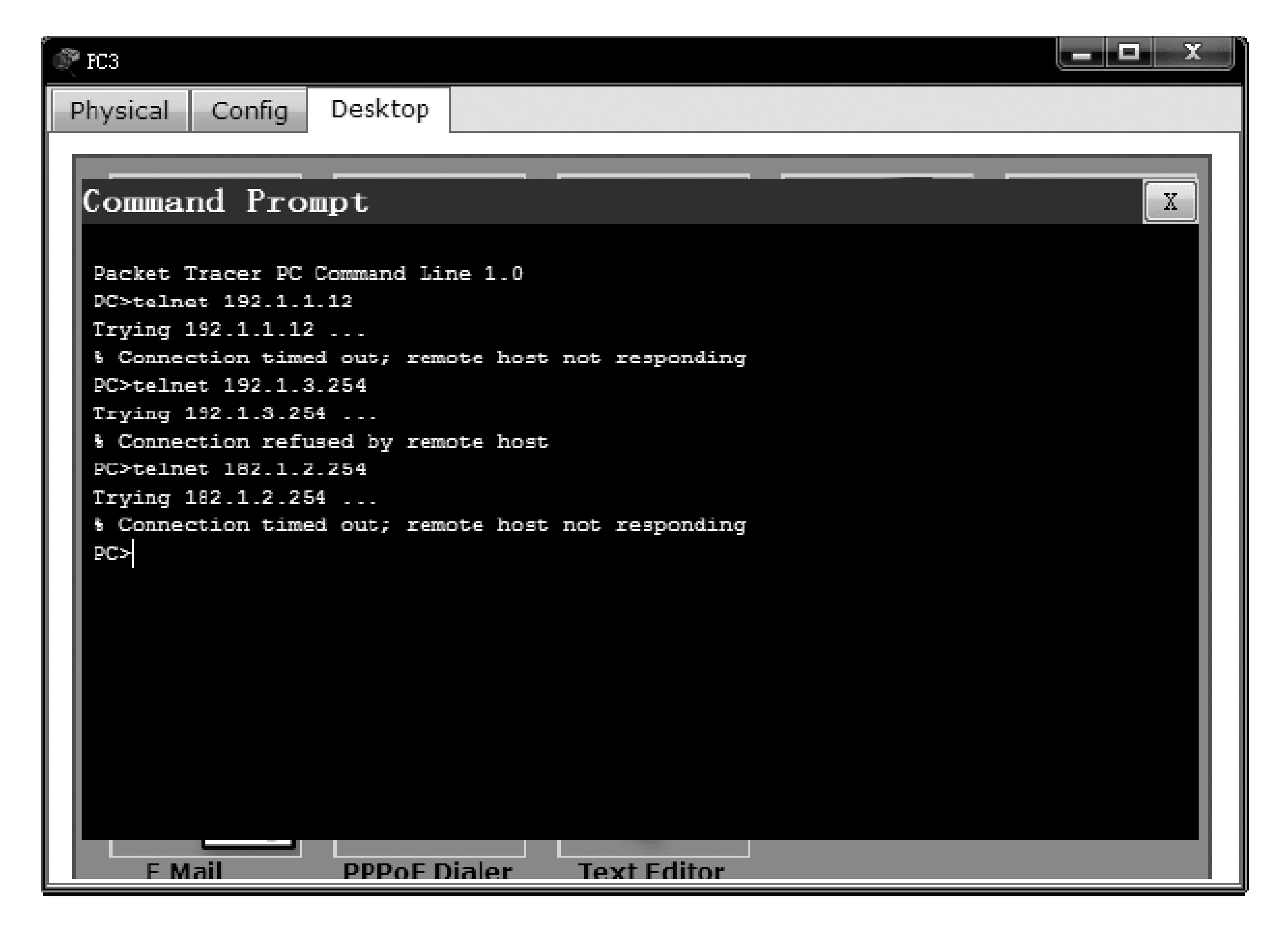


图 3.18　PC3 远程配置失败界面

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name vlan4
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,3,4
Switch(config-if)#exit
Switch(config)#enable password ccc        (配置进入全局模式口令 ccc)
Switch(config)#line vty 0 15              (进入虚拟端口配置模式)
Switch(config-line)#password ccc          (配置远程配置口令 ccc)
Switch(config-line)#exit
Switch(config)#interface vlan 1           (进入 VLAN 1 对应的 IP 接口配置模式)
Switch(config-if)#ip address 192.1.1.13 255.255.255.0
                                          (配置设备管理地址)
Switch(config-if)#no shutdown
                              (开启 VLAN 1 对应的 IP 接口,允许其他终端访问设备管理地址)
Switch(config-if)#exit
```

Switch1 和 Switch2 命令行配置过程与此相似,不再赘述。

（2）三层交换机 Switch4 命令行配置过程。

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 2
Switch(config-vlan)#name vlan2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name vlan4
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport trunk encapsulation dot1q      (配置标记端口封装方式)
Switch(config-if)#switchport mode trunk                     (将端口配置为标记端口)
Switch(config-if)#switchport trunk allowed vlan 1,2
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,2,3
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1,3,4
Switch(config-if)#exit
Switch(config)#enable password ddd
Switch(config)#interface vlan 2
Switch(config-if)#ip address 192.1.2.254 255.255.255.0
                                      (配置 VLAN2 对应的 IP 接口的 IP 地址和子网掩码)
Switch(config-if)#exit
Switch(config)#interface vlan 3
Switch(config-if)#ip address 192.1.3.254 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 4
Switch(config-if)#ip address 192.1.4.254 255.255.255.0
Switch(config-if)#exit
Switch(config)#access-list 1 permit 192.1.2.0 0.0.0.255
          (配置只处理源 IP 地址属于网络地址 192.1.2.0/24 的 IP 分组的标准访问控制列表)
Switch(config)#access-list 1 deny any
Switch(config)#line vty 0 15                                (进入虚拟终端配置模式)
Switch(config-line)#password ddd                            (配置远程配置口令 ddd)
Switch(config-line)#access-class 1 in
                                (通过编号为 1 的标准访问列表指定允许远程配置的终端范围)
```

```
Switch(config-line)#exit
```

3.3.2 简单互连网远程设备配置实验

1. 实验内容

(1) 完成简单互连网设计和配置。

(2) 配置二层交换机管理地址。

(3) 验证设备远程配置过程。

2. 网络结构

简单互连网结构如图 3.19 所示。由两个路由器互连的 3 个以太网组成,三个以太网的网络地址分别为 192.1.1.0/24、192.1.2.0/24 和 192.1.3.0/24。S1、S2 和 S3 的管理地址分别属于这三个网络地址,路由器任何一个接口的 IP 地址都可作为管理地址。要求只允许终端 A 远程配置简单互连网络中的网络设备。

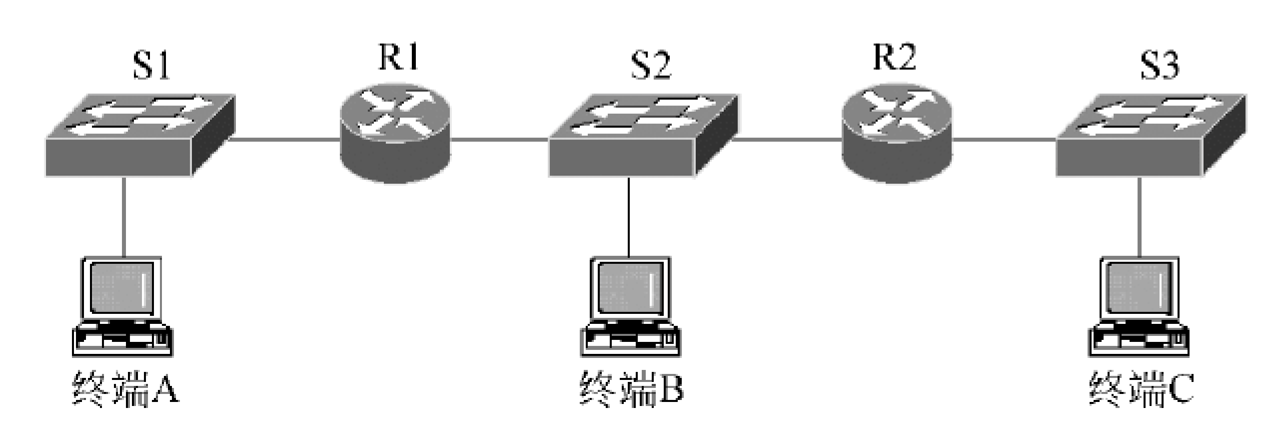


图 3.19　简单互连网结构

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 3.19 所示的网络结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图 3.20 所示。

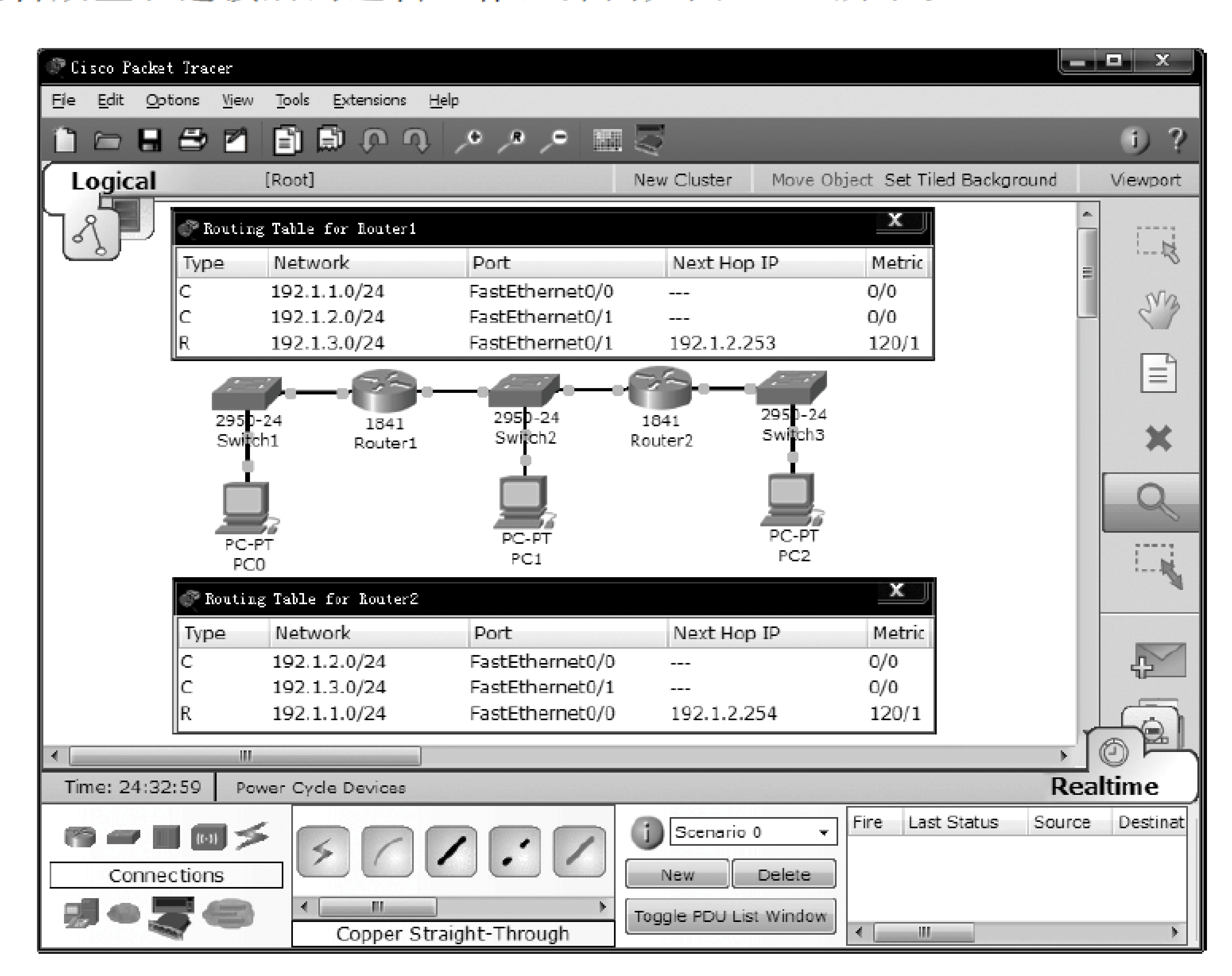


图 3.20　放置和连接设备后的逻辑工作区界面及路由表

(2) 为路由器接口配置 IP 地址和子网掩码，Router1 接口配置界面如图 3.21 所示，路由器所有接口的 IP 地址都是路由器的设备管理地址。配置参与 RIP 建立动态路由项的网络的网络地址，Router1 RIP 配置界面如图 3.22 所示。建立动态路由项后的 Router1 和 Router2 的路由表如图 3.20 所示。

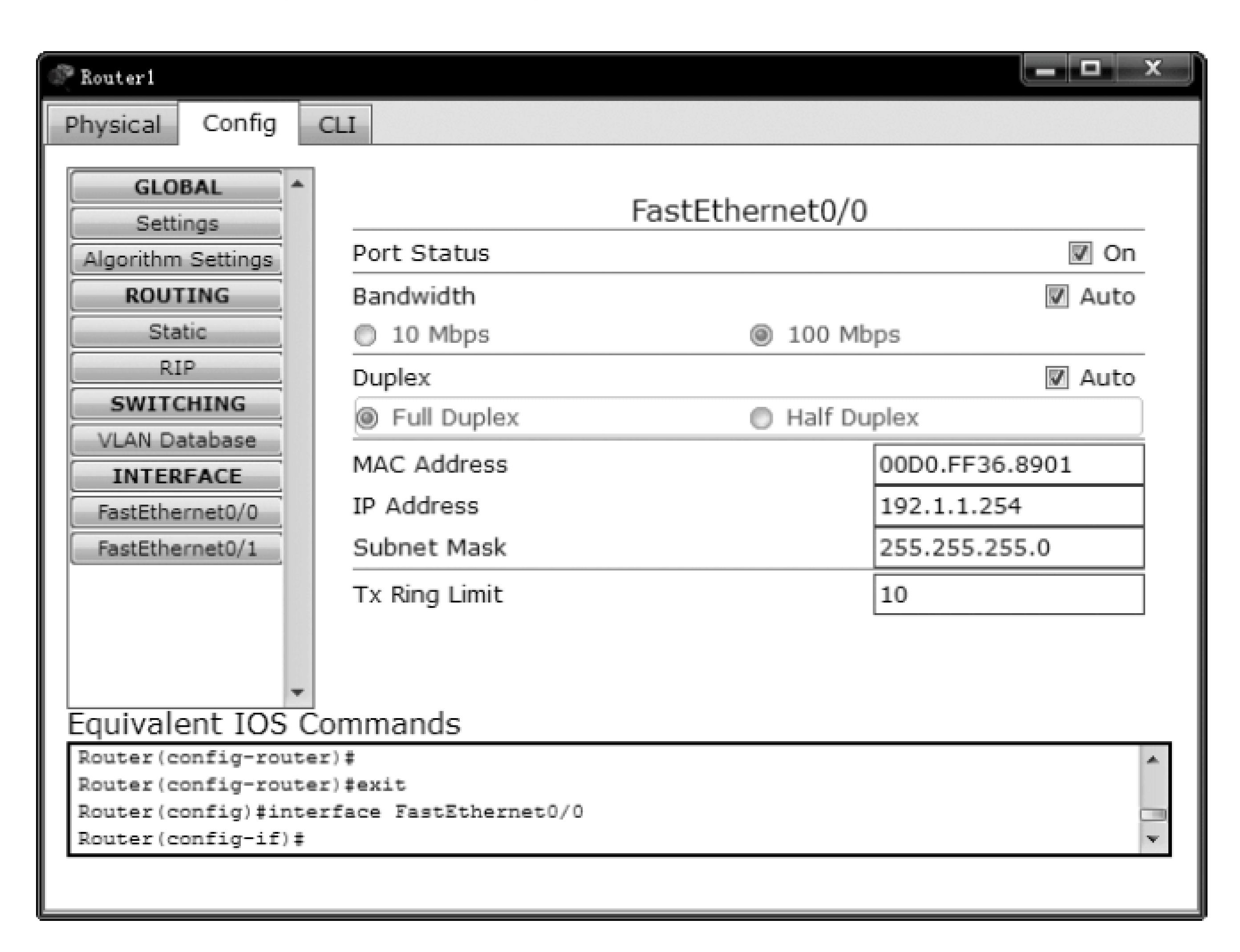


图 3.21　路由器接口配置界面

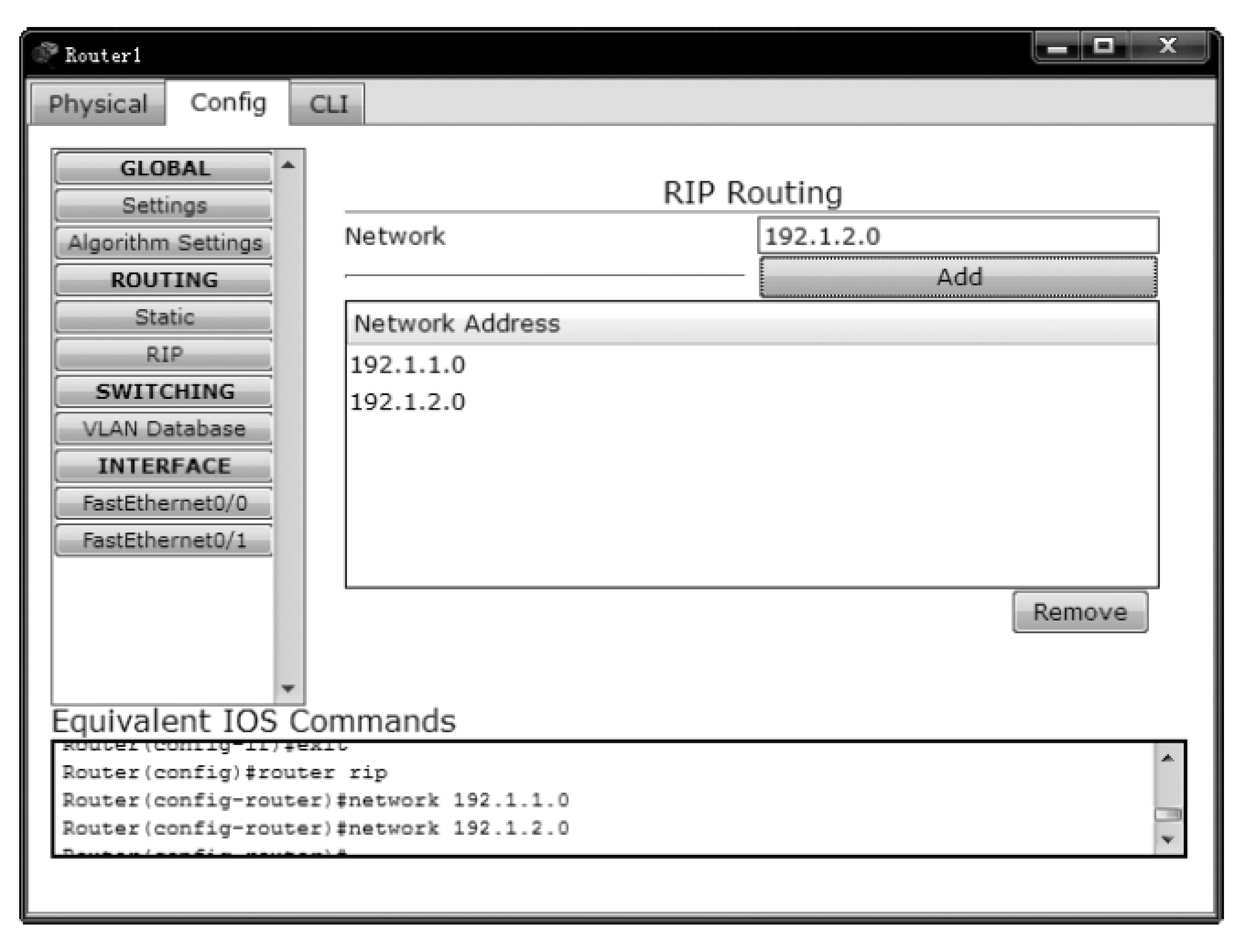


图 3.22　路由器 RIP 配置界面

(3) 通过命令为二层交换机配置管理地址和默认网关地址，管理地址必须与交换机所在网络的网络地址一致，默认网关地址是连接该网络的路由器接口的 IP 地址，如 Switch2 位于网络 192.1.2.0/24，其管理地址为 192.1.2.10，默认网关地址为 192.1.2.254。

(4) 配置访问控制列表,使得二层交换机和路由器的虚拟终端只允许输入源 IP 地址为 192.1.1.1/32 的 IP 分组。PC0 配置的网络信息如图 3.23 所示,允许 PC0 远程配置二层交换机和路由器,PC0 远程配置网络设备的界面如图 3.24 所示。由于 PC1 配置的 IP 地址为 192.1.2.1,如图 3.25 所示,因此无法远程配置网络设备,PC1 远程配置网络设备失败的界面如图 3.26 所示。

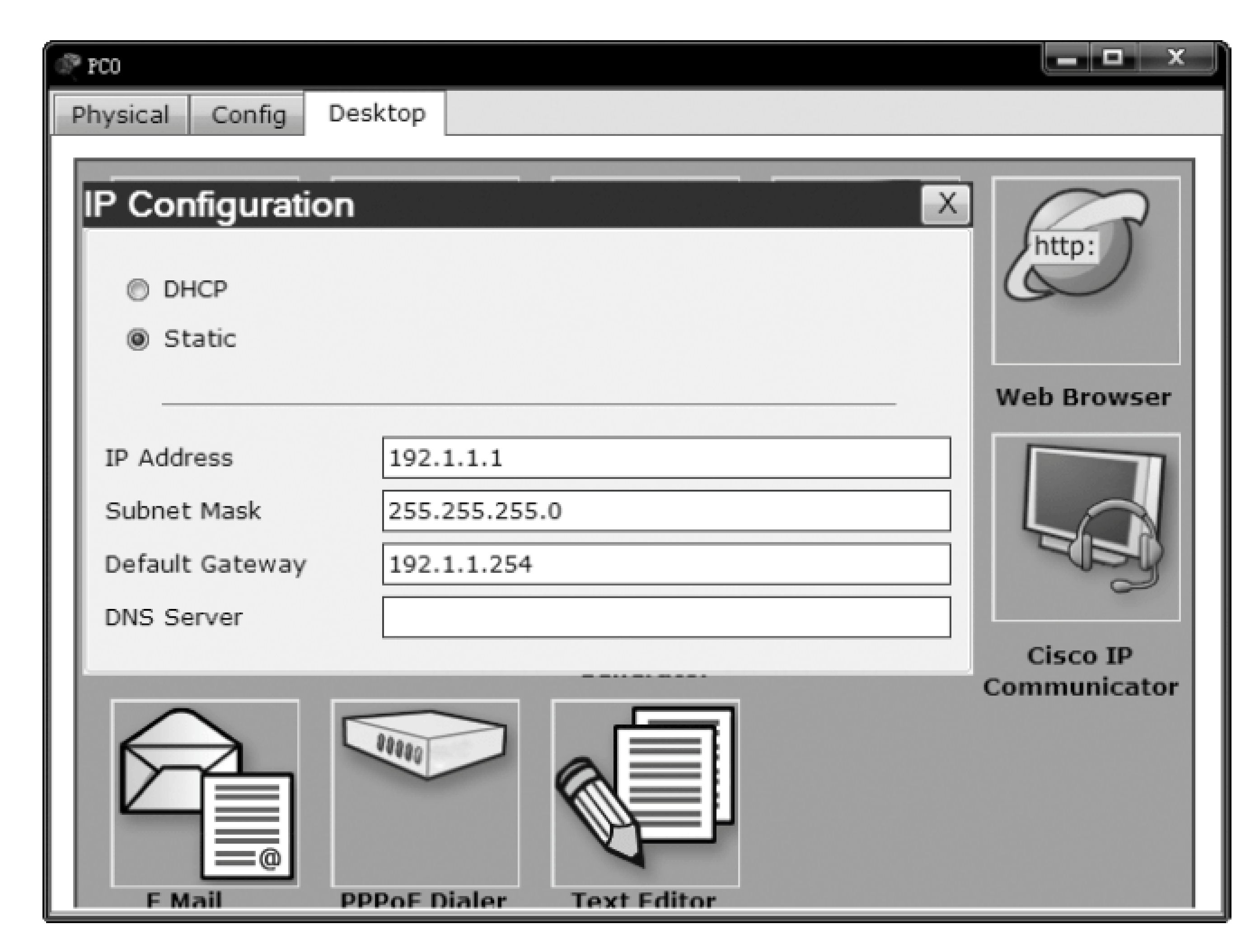


图 3.23　PC0 配置的网络信息

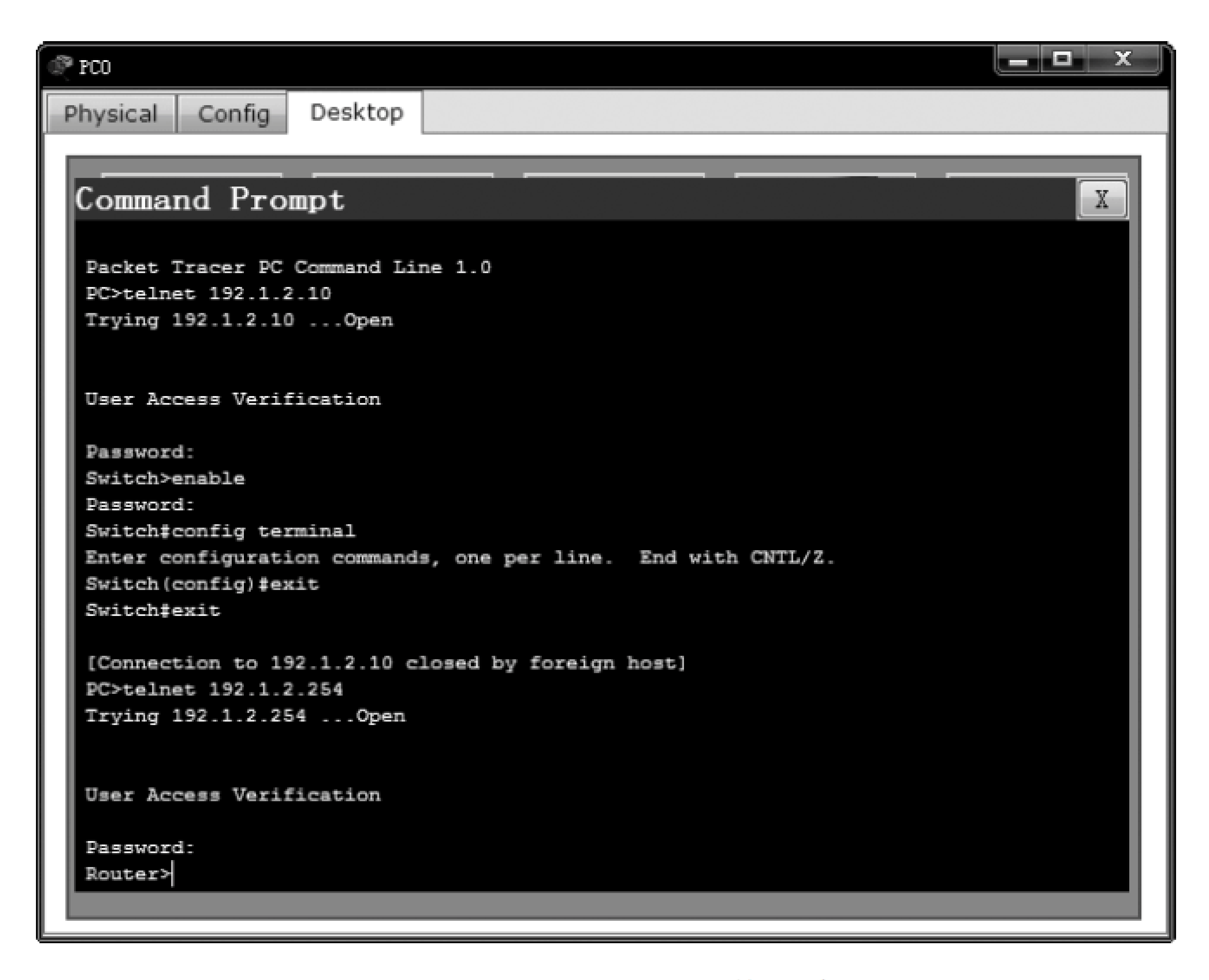


图 3.24　PC0 远程配置网络设备界面

4. 命令行配置过程

(1) Switch2 命令行配置过程。

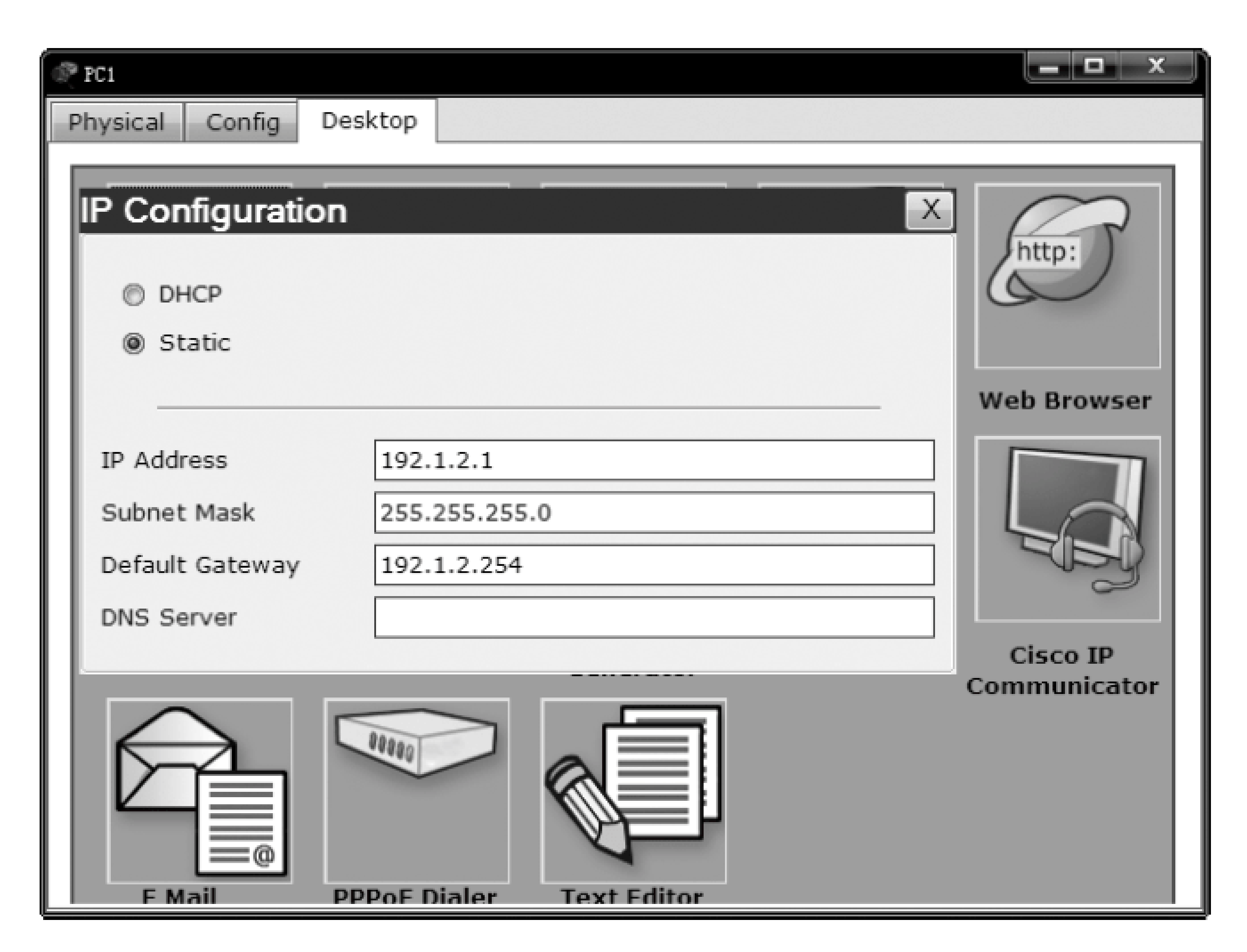


图 3.25 PC1 配置的网络信息

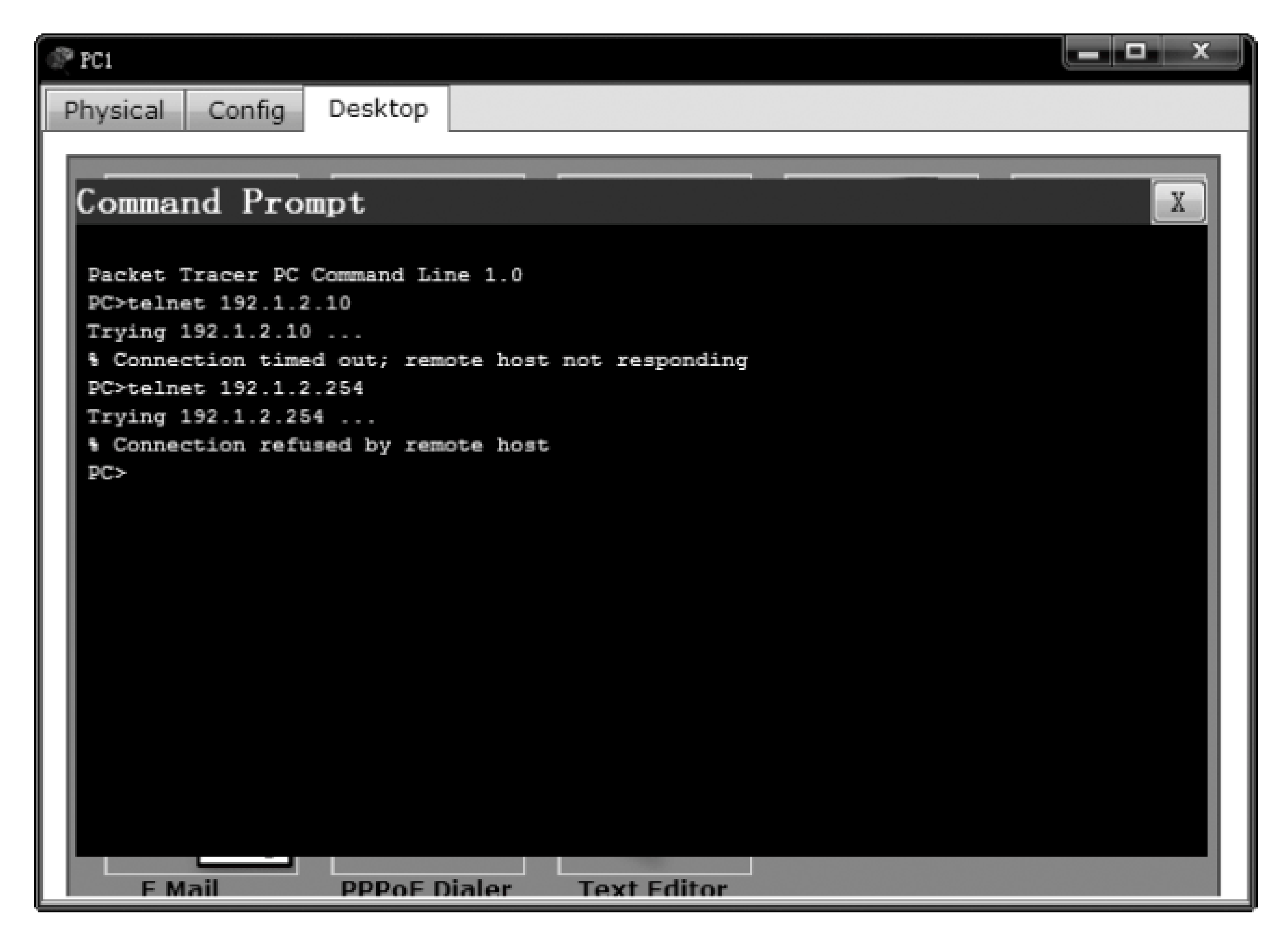


图 3.26 PC1 远程配置网络设备失败的界面

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.1.2.10 255.255.255.0 (配置管理地址)
Switch(config-if)#no shutdown                         (开启 VLAN 1 对应的 IP 接口)
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.1.2.254
                     (配置默认网关地址,它必须是连接交换机所在网络的路由器接口的 IP 地址)
Switch(config)#enable password bbb                    (配置进入全局配置模式的口令)
Switch(config)#access-list 1 permit host 192.1.1.1
```

```
                    (配置只允许处理源 IP 地址为 192.1.1.1/32 的 IP 分组的标准访问控制列表)
Switch(config)#access-list 1 deny any
Switch(config)#line vty 0 15                    (进入虚拟终端配置模式)
Switch(config-line)#password bbb                (配置远程配置口令)
Switch(config-line)#access-class 1 in
                    (只允许符合编号为 1 的标准访问控制列表的 IP 分组进入虚拟终端)
Switch(config-line)#exit
```

Switch1 和 Switch3 命令行配置过程与此相似，不再赘述。

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.253 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip                       (进入 RIP 配置过程)
Router(config-router)#network 192.1.2.0
                    (配置参与 RIP 建立动态路由项的网络的网络地址)
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#enable password eee              (配置进入全局配置模式的口令)
Router(config)#access-list 1 permit host 192.1.1.1
                    (配置只允许处理源 IP 地址为 192.1.1.1/32 的 IP 分组的标准访问控制列表)
Router(config)#access-list 1 deny any
Router(config)#line vty 0 15                    (进入虚拟终端配置模式)
Router(config-line)#password eee                (配置远程配置口令)
Router(config-line)#access-class 1 in
                    (只允许符合编号为 1 的标准访问控制列表的 IP 分组进入虚拟终端)
Router(config-line)#exit
```

Router1 命令行配置过程与此相似，不再赘述。

5. 终端通过 SSH 远程配置路由器过程

(1) 实现过程。

终端通过 Telnet 对网络设备进行远程配置的方式存在安全隐患，主要原因在于：一是用明文方式传输口令；二是通过 IP 分组的源 IP 地址进行源端鉴别。为了解决远程配置过程中的安全问题，采用安全 Shell(Secure Shell，SSH)作为远程配置协议。SSH 一是通过证书或共享密钥进行源端鉴别；二是对口令进行加密传输。采用 SSH 对路由器实施远程配置的步骤如下：

① 在全局配置模式,通过命令“hostname 主机名”为路由器配置主机名。
② 在全局配置模式,通过命令“ip domain－name 域名”为网络配置域名。
③ 在全局配置模式,通过命令“crypto key generate rsa”产生不对称密钥对。
④ 在全局配置模式,通过命令“username 用户名 password 口令”创建本地用户。
⑤ 在虚拟终端配置模式,通过命令“login local”指定用本地用户鉴别登录用户。
⑥ 在虚拟终端配置模式,通过命令“transport input ssh”指定用 SSH 作为远程配置协议。
⑦ PC0 通过启动 SSH 客户端开始远程配置过程,SSH 客户端配置界面如图 3.27 所示。

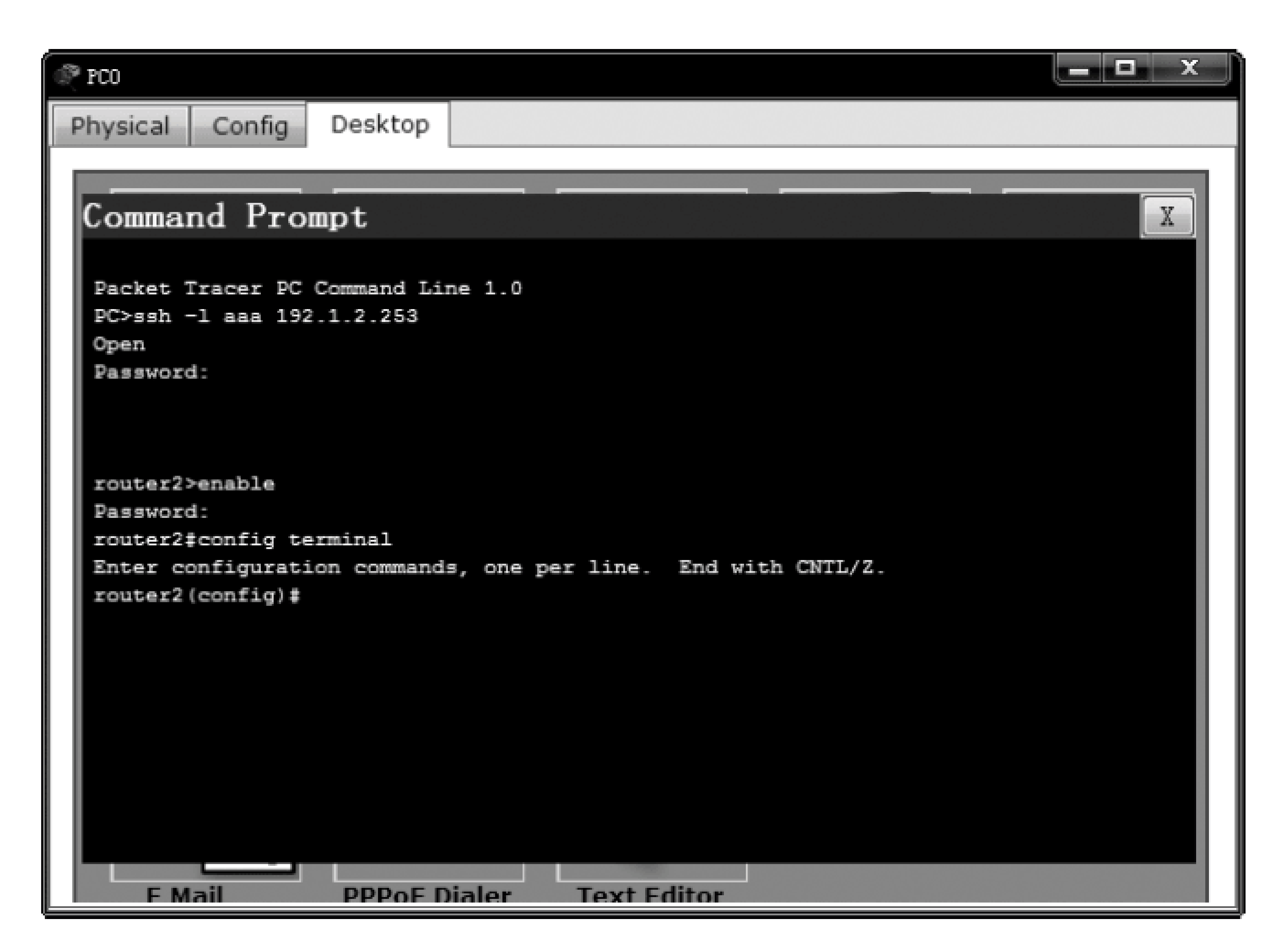


图 3.27 PC0 SSH 远程配置 Router2 界面

值得指出的是,配置主机名、域名,产生不对称密钥对的作用是允许 Router2 作为 SSH 客户端远程访问其他网络设备,这种情况下,其他网络设备通过证书和 Router2 的公钥鉴别 Router2 的身份。

(2) Router2 命令行配置过程。

```
Router(config)#hostname router2                          (配置主机名 Router2)
router2(config)#ip domain-name abc.com.cn                (配置域名 abc.com.cn)
router2(config)#crypto key generate rsa                  (生成不对称密钥对)
How many bits in the modulus [512]:                      (选择 512 位为 RSA 密钥长度)
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
router2(config)#username aaa password bbb        (生成用户名为 aaa、口令为 bbb 的本地用户)
router2(config)#line vty 0 15
router2(config-line)#login local                         (用本地用户库鉴别登录用户)
router2(config-line)#transport input ssh                 (指定 SSH 作为传输协议)
router2(config-line)#exit
```

3.3.3　交换机端口配置实验

1. 实验内容

（1）安全端口配置。

（2）端口全双工方式配置。

2. 网络结构

为了防止黑客在两个交换机之间插入集线器，将互连交换机的端口固定设置为全双工通信方式，如果将集线器接入全双工通信方式的端口，该端口将关闭。为了控制终端接入，通过配置访问控制列表，将每一个交换机端口和 MAC 地址绑定，同时将交换机端口固定设置为全双工通信方式，以此保证每一个交换机端口只允许接入单个 MAC 地址等于访问控制列表中与该端口绑定的 MAC 地址的终端。

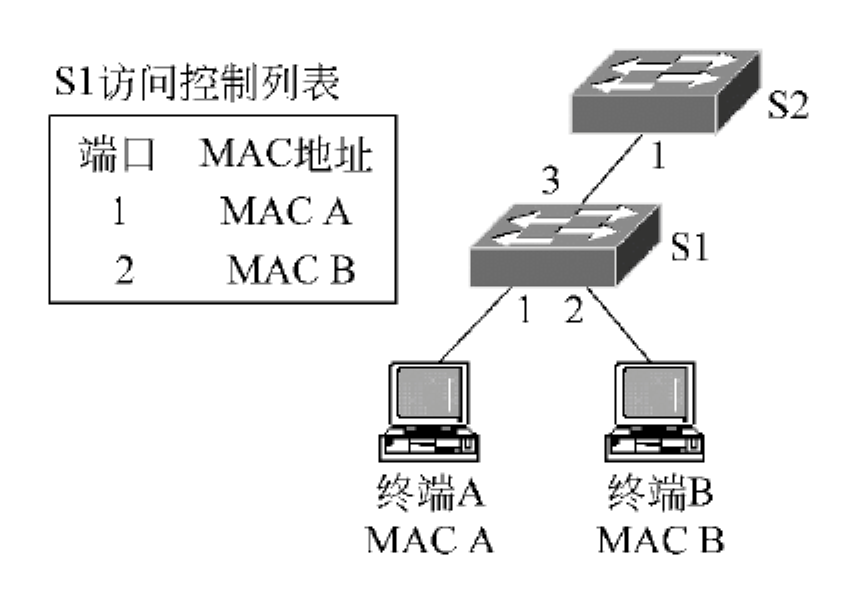


图 3.28　交换机端口配置方式

3. 实验步骤

（1）启动 Packet Tracer，在逻辑工作区根据图 3.28 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 3.29所示。

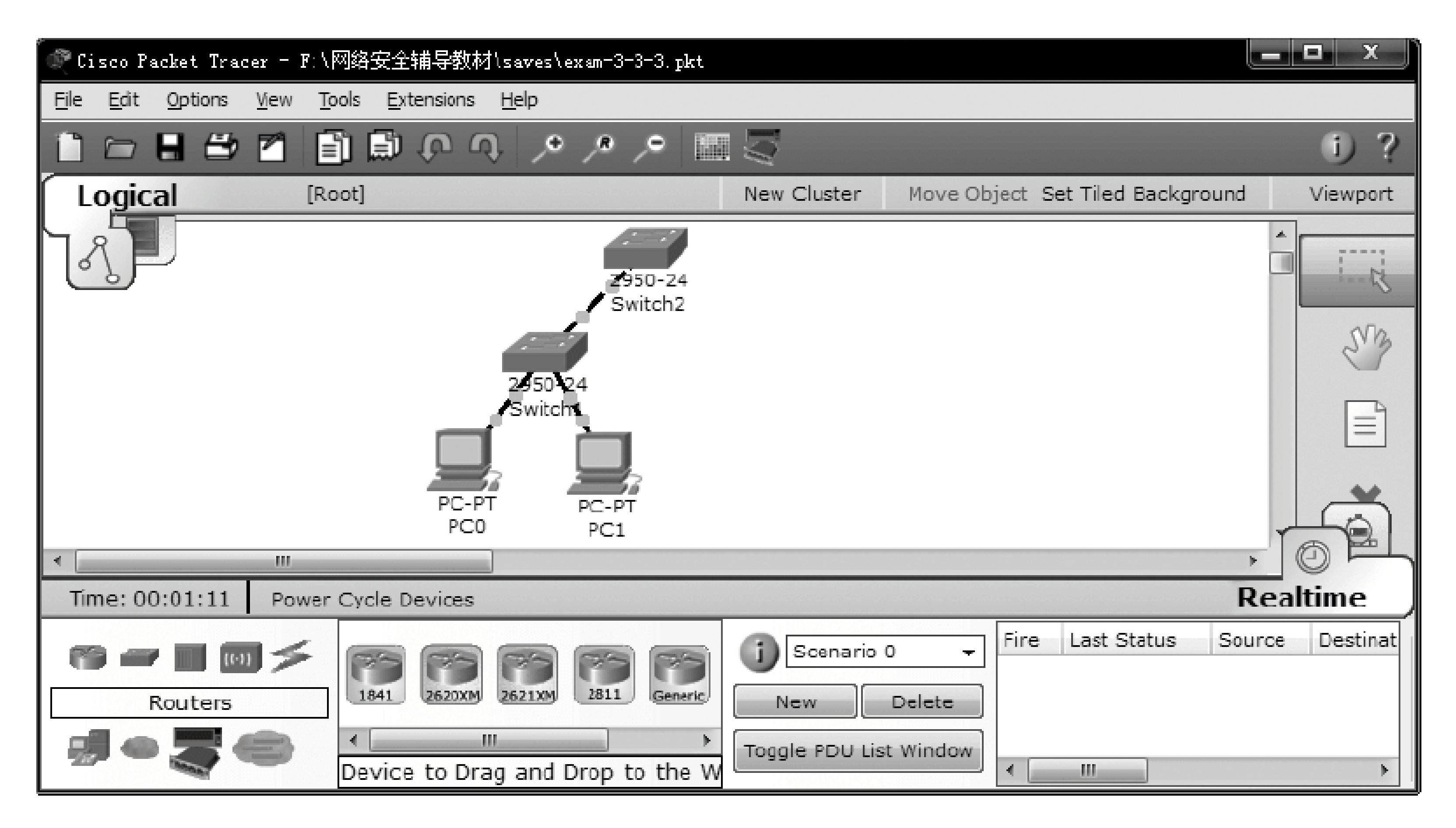


图 3.29　放置和连接设备后的逻辑工作区界面

（2）通过命令将交换机 Switch2 端口 FastEthernet0/1 配置成全双工通信方式，通过命令将交换机 Switch1 端口 FastEthernet0/1、FastEthernet0/2 和 FastEthernet0/3 配置成全双工通信方式，将端口 FastEthernet0/1 和 FastEthernet0/2 配置成安全端口，并且分别和 PC0、PC1 的 MAC 地址绑定。

4. 命令行配置过程

（1）Switch1 命令行配置过程。

```
Switch>enable
Switch#configure terminal
```

```
Switch(config)#interface FastEthernet0/3
Switch(config-if)#duplex full                          (将端口配置成全双工通信方式)
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#duplex full
Switch(config-if)#switchport mode access               (将端口配置成非标记端口模式)
Switch(config-if)#switchport port-security             (开启安全端口功能)
Switch(config-if)#switchport port-security maximum 1
                                                       (将端口允许绑定的 MAC 地址数配置为 1)
Switch(config-if)#switchport port-security mac-address 0050.0F70.ED27
                              (将端口和 MAC 地址 0050.0F70.ED27 绑定在一起,表示只允许
                               源 MAC 地址为 0050.0F70.ED27 的 MAC 帧进入该端口)
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0060.3EED.8526
Switch(config-if)#exit
```

(2) Switch2 命令行配置过程。

```
Switch>enable
Switch#configure terminal
Switch(config)#interface FastEthernet0/1
Switch(config-if)#duplex full                          (将端口配置成全双工通信方式)
Switch(config-if)#exit
```

3.3.4 访问控制和流量管制实验

1. 实验内容

(1) 完成网络配置。

(2) 完成路由器 CBAC 配置。

(3) 完成路由器流量管制器配置。

2. 网络结构

图 3.30 所示是一个简化了的企业网结构。为了保证网络安全,一是要求对外部网络终端访问非军事区中的服务器的过程实施严格控制,包括限制外部网络终端发起的、与非军事区中服务器之间未完成的 TCP 连接数量,以应对黑客终端发起的 SYN 泛洪攻击;二是为了防止邮件病毒快速扩散,需要限制发送邮件的流量;三是为了防止内部网络终端对非军事区中服务器发起拒绝服务攻击,限制内部网络进入非军事区的 ICMP 报文流量。因此,对图 3.30 所示网络实施以下访问控制策略。

① 允许内部网络终端访问非军事区中的 E-mail 服务器和 Web 服务器。

② 允许内部网络终端通过 ICMP 管理和检测非军事区中的 E-mail 服务器和 Web 服务器。

③ 允许外部网络终端访问非军事区中的 Web 服务器。

④ 允许非军事区中的 E-mail 服务器和外部网络中的 E-mail 服务器通过 SMTP 相互访问。

⑤ 对内部网络进入非军事区的 ICMP 和 SMTP 报文流量进行管制。

⑥ 对外部网络进入非军事区的 SMTP 报文流量进行管制。

⑦ 限制外部网络终端发起的、与非军事区中服务器之间未完成的 TCP 连接数量。

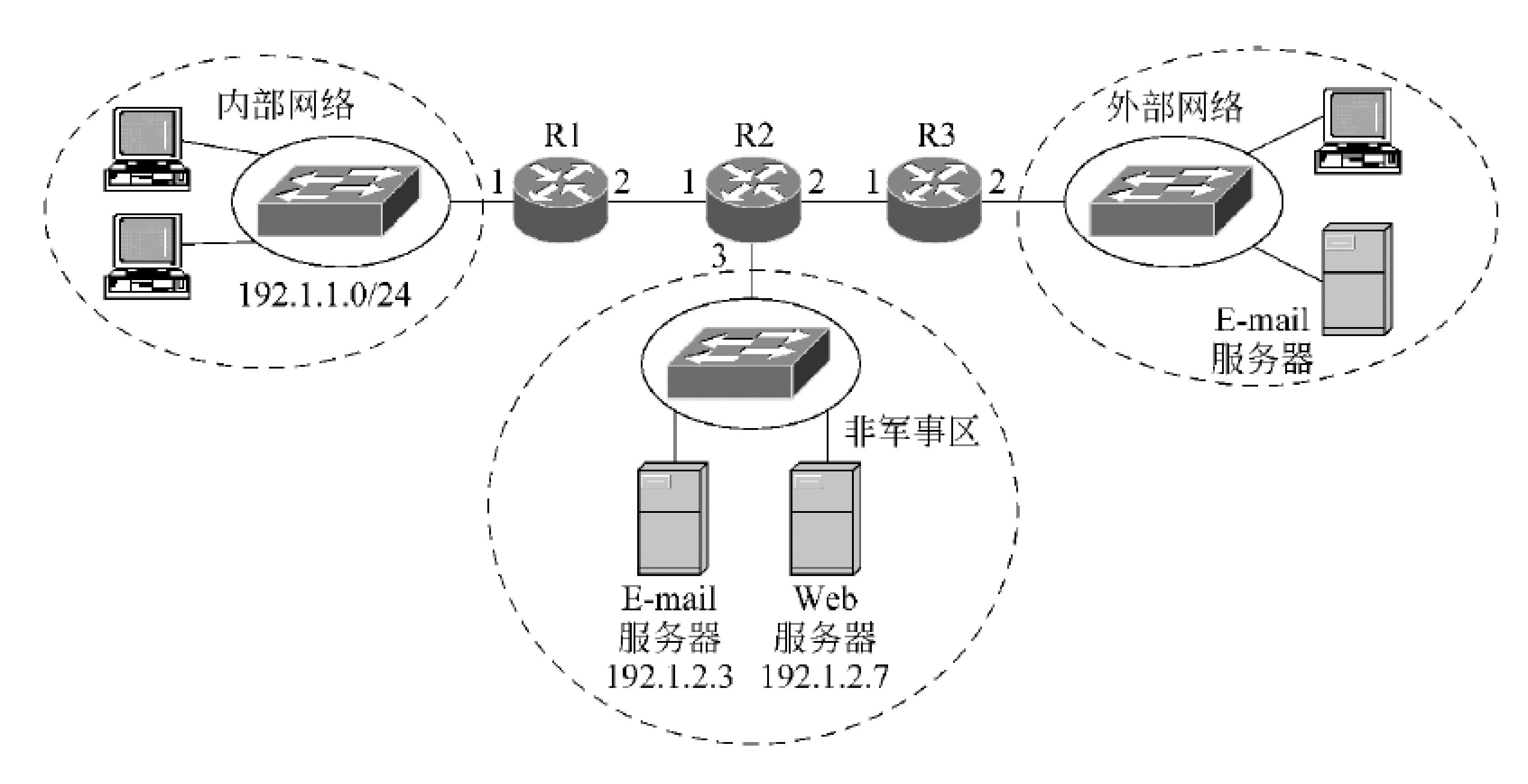


图 3.30　简化了的企业网结构

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 3.30 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 3.31 所示。

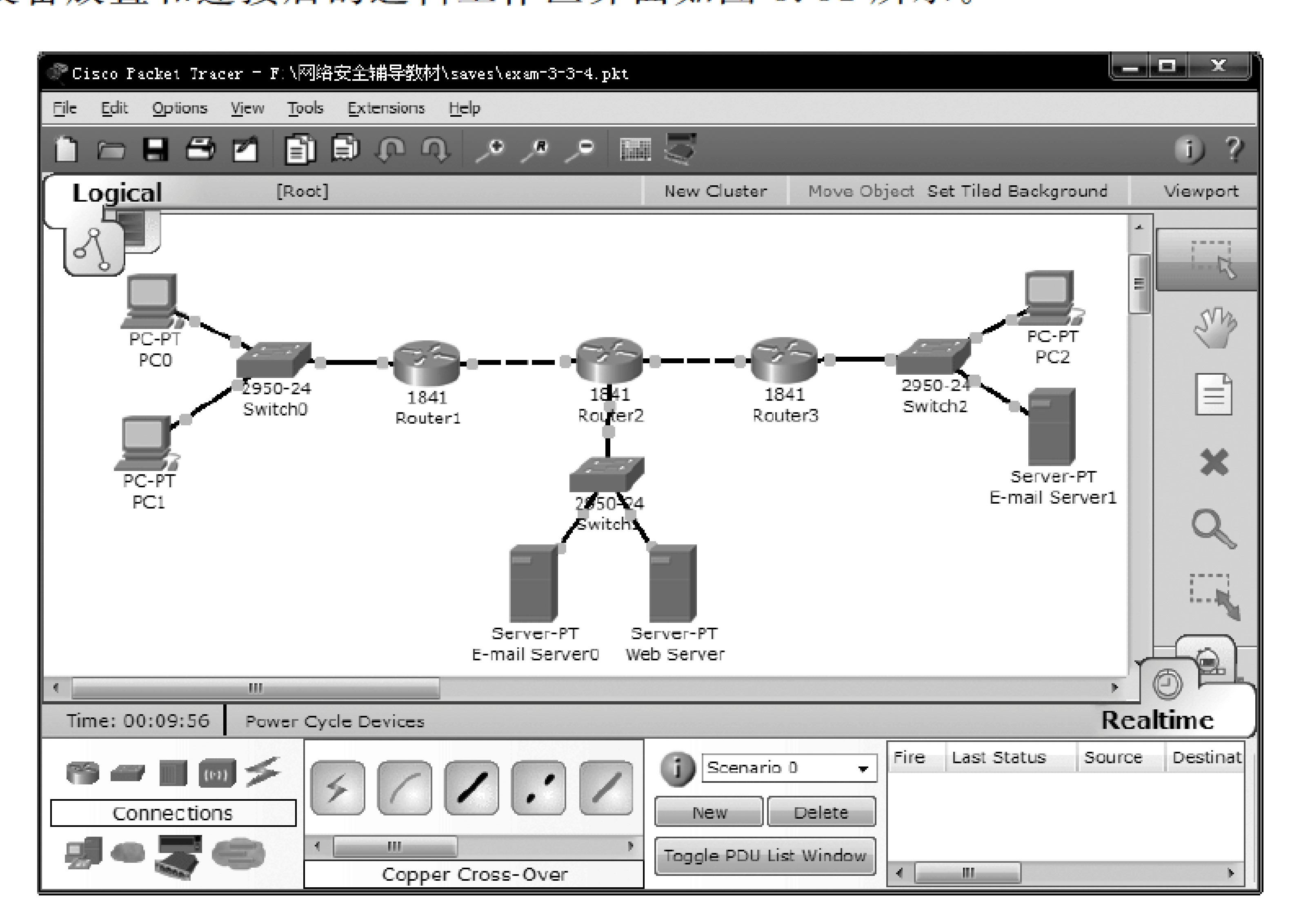


图 3.31　放置和连接设备后的逻辑工作区界面

(2) 完成路由器各个接口的配置和RIP配置,建立完整的路由表,各个路由器建立的完整路由表如图3.32所示。这里假定内部网络的网络地址为192.1.1.0/24,非军事区的网络地址为192.1.2.0/24,外部网络的网络地址为192.1.3.0/24。互连Router1和Router2的网络的网络地址为192.1.4.0/24,Router1和Router2连接交叉双绞线缆的两个接口的IP地址分别是192.1.4.1和192.1.4.2。互连Router2和Router3的网络的网络地址为192.1.5.0/24,Router2和Router3连接交叉双绞线缆的两个接口的IP地址分别是192.1.5.1和192.1.5.2。

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	192.1.1.0/24	FastEthernet0/0	---	0/0
C	192.1.4.0/24	FastEthernet0/1	---	0/0
R	192.1.2.0/24	FastEthernet0/1	192.1.4.2	120/1
R	192.1.3.0/24	FastEthernet0/1	192.1.4.2	120/2
R	192.1.5.0/24	FastEthernet0/1	192.1.4.2	120/1

(a) Router1路由表

Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet1/0	---	0/0
C	192.1.4.0/24	FastEthernet0/0	---	0/0
C	192.1.5.0/24	FastEthernet0/1	---	0/0
R	192.1.1.0/24	FastEthernet0/0	192.1.4.1	120/1
R	192.1.3.0/24	FastEthernet0/1	192.1.5.2	120/1

(b) Router2路由表

Routing Table for Router3

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	FastEthernet0/1	---	0/0
C	192.1.5.0/24	FastEthernet0/0	---	0/0
R	192.1.1.0/24	FastEthernet0/0	192.1.5.1	120/2
R	192.1.2.0/24	FastEthernet0/0	192.1.5.1	120/1
R	192.1.4.0/24	FastEthernet0/0	192.1.5.1	120/1

(c) Router3路由表

图3.32 路由器路由表

(3) 根据制定的访问控制策略,路由器R1接口1输入方向只允许进入与内部网络终端发起访问非军事区中服务器和外部网络中Web服务器相关的TCP报文,以及内部网络终端用ICMP管理非军事区中服务器相关的ICMP报文。路由器R1接口1输出方向除了与上述访问过程相关的响应报文进入内部网络外,禁止其他一切IP分组进入内部网络。路由器R1接口2输出方向限制内部网络终端发送的SMTP和ICMP报文的流量。

(4) 根据制定的访问控制策略,路由器R2接口3输出方向只允许与内部网络终端和外部网络终端发起访问非军事区中服务器相关的TCP报文进入非军事区,以及内部网络终端用ICMP管理非军事区中服务器相关的ICMP报文进入非军事区。路由器R2接口3输入方向除了与上述访问过程相关的响应报文离开非军事区外,还允许与非军事区中E-mail服务器发起访问外部网络中E-mail服务器相关的TCP报文离开非军事区。与此对应,路由器R2接口3输出方向需要允许该访问过程对应的响应报文进入非军事区。

(5) 根据制定的访问控制策略,路由器R3接口2输入方向只允许进入与外部网络终端发起访问非军事区中服务器相关的TCP报文、作为内部网络终端访问外部网络中Web服务器产生的响应报文的TCP报文,以及非军事区中E-mail服务器访问外部网络

中 E-mail 服务器产生的响应报文的 TCP 报文。同时，路由器 R3 接口 1 输出方向限制外部网络进入的 SMTP 报文的流量。可以开放路由器 R3 接口 2 输出方向。

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router(config)#ip inspect max-incomplete high 100
                                    (设置路由器检测到的未完成的 TCP 连接上限)
Router(config)#ip inspect max-incomplete low 50
                                    (设置路由器检测到的未完成的 TCP 连接下限)
Router(config)#ip inspect name a1 icmp          (配置名为 a1 的检测器,检测 ICMP 和 TCP 报文)
Router(config)#ip inspect name a1 tcp
Router(config)#access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
                                 (配置允许网络 192.1.1.0/24 中的终端用 SMTP 访问
                                  IP 地址为 192.1.2.3 的邮件服务器的过滤规则)
Router(config)#access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq pop3
                                 (配置允许网络 192.1.1.0/24 中的终端用 POP3 访问
                                  IP 地址为 192.1.2.3 的邮件服务器的过滤规则)
Router(config)#access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www
                                 (配置允许网络 192.1.1.0/24 中的终端用 HTTP 访问
                                  IP 地址为 192.1.2.7 的 Web 服务器的过滤规则)
Router(config)#access-list 101 permit tcp 192.1.1.0 0.0.0.255 any eq www
          (配置允许网络 192.1.1.0/24 中的终端用 HTTP 访问外部网络中 Web 服务器的过滤规则)
Router(config)#access-list 101 permit icmp 192.1.1.0 0.0.0.255 host 192.1.2.3
                                 (配置允许网络 192.1.1.0/24 中的终端用 ICMP 管理
                                  IP 地址为 192.1.2.3 的邮件服务器的过滤规则)
Router(config)#access-list 101 permit icmp 192.1.1.0 0.0.0.255 host 192.1.2.7
                                 (配置允许网络 192.1.1.0/24 中的终端用 ICMP 管理
                                  IP 地址为 192.1.2.7 的 Web 服务器的过滤规则)
Router(config)#access-list 101 deny ip any any      (配置拒绝一切 IP 分组的过滤规则)
Router(config)#access-list 102 deny ip any any
Router(config)#access-list 103 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
Router(config)#access-list 103 permit icmp 192.1.1.0 0.0.0.255 host 192.1.2.3
Router(config)#access-list 103 permit icmp 192.1.1.0 0.0.0.255 host 192.1.2.7
Router(config)#access-list 103 deny ip any any
Router(config)#class-map smtpicmp           (定义名为 smtpicmp 的分类器)
Router(config-cmap)#match access-group 103        (分类标准是编号为 103 的访问控制列表)
Router(config-cmap)#exit
Router(config)#policy-map smtpicmp          (定义名为 smtpicmp 的流量管制器)
Router(config-pmap)#class smtpicmp          (由名为 smtpicmp 的分类器对信息流分类)
Router(config-pmap-c)#shape average 8000(将分类器指定的信息流的流量限制在 8kbps)
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 101 in
```

```
                    (允许编号为 101 的访问控制列表指定的 TCP 和 ICMP 报文离开内部网络)
Router(config-if)#ip access-group 102 out
                                       (初始情况下,拒绝一切 IP 分组进入内部网络)
Router(config-if)#ip inspect a1 in
      (允许作为编号为 101 的访问控制列表指定的 TCP 和 ICMP 报文的响应报文进入内部网络)
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#service-policy output smtpicmp            (在输出端口设置流量管制器)
Router(config-if)#exit
```

(2) Router2 命令行配置过程。

```
Router(config)#access-list 101 permit icmp 192.1.1.0 0.0.0.255 host 192.1.2.3
Router(config)#access-list 101 permit icmp 192.1.1.0 0.0.0.255 host 192.1.2.7
Router(config)#access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq pop3
Router(config)#access-list 101 permit tcp any host 192.1.2.3 eq smtp
Router(config)#access-list 101 permit tcp any host 192.1.2.7 eq www
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 permit tcp host 192.1.2.3 any eq smtp
Router(config)#access-list 102 deny ip any any
Router(config)#ip inspect name a1 icmp
Router(config)#ip inspect name a1 tcp
Router(config)#ip inspect name a2 tcp
Router(config)#interface FastEthernet1/0
Router(config-if)#ip access-group 101 out
Router(config-if)#ip access-group 102 in
Router(config-if)#ip inspect a1 out
Router(config-if)#ip inspect a2 in
Router(config-if)#exit
```

(3) Router3 命令行配置过程。

```
Router(config)#ip inspect max-incomplete high 100
Router(config)#ip inspect max-incomplete low 50
Router(config)#access-list 101 permit tcp any host 192.1.2.3 eq smtp
Router(config)#access-list 101 permit tcp any host 192.1.2.7 eq www
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 permit tcp host 192.1.2.3 any eq smtp
Router(config)#access-list 102 permit tcp 192.1.1.0 0.0.0.255 any eq www
Router(config)#access-list 102 deny ip any any
Router(config)#access-list 103 permit tcp any host 192.1.2.3 eq smtp
Router(config)#access-list 103 deny ip any any
Router(config)#class-map smtp
Router(config-cmap)#match access-group 103
Router(config-cmap)#exit
Router(config)#policy-map smtp
```

```
Router(config-pmap)#class smtp
Router(config-pmap-c)#shape average 8000
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#ip inspect name a1 tcp
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 101 out
Router(config-if)#ip access-group 102 in
Router(config-if)#ip inspect a1 in
Router(config-if)#ip inspect a1 out
Router(config-if)#service-policy output smtp
Router(config-if)#exit
```

3.3.5　安全路由实验

1. 实验内容

(1) OSPF 配置过程。

(2) 路由消息鉴别。

(3) 验证防路由项欺骗攻击机制。

2. 网络结构

路由项欺骗攻击过程如图 3.33 所示。入侵路由器伪造了和网络 192.1.4.0/24 直接相连的链路状态信息,导致路由器 R1 通过 OSPF 生成的动态路由项发生错误,如图 3.33 中 R1 错误路由表。解决路由项欺骗攻击问题的关键有三点:一是对建立邻接关系的路由器身份进行鉴别,只和授权路由器建立邻接关系;二是对相互交换的链路状态信息进行完整性检测,只接收和处理完整性检测通过的链路状态信息;三是通过链路状态信息中携

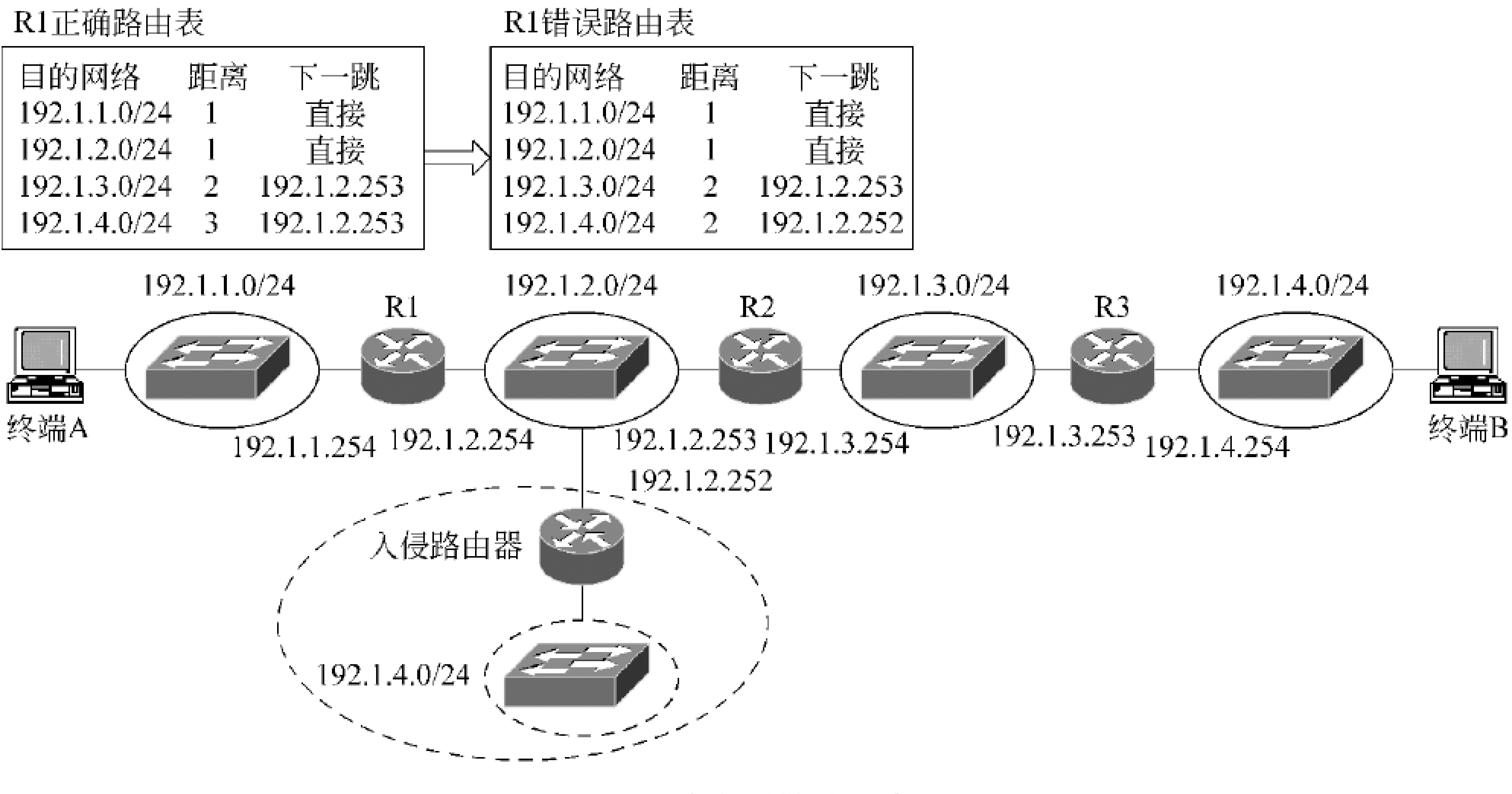


图 3.33　路由项欺骗攻击过程

带的序号确定该链路状态信息不是黑客截获后重放的链路状态信息。实现这一功能的基础是在相邻路由器中配置相同的共享密钥,相互交换的链路状态信息和 Hello 报文携带由共享密钥加密的序号和由共享密钥生成的消息鉴别码(Message Authentication Code,MAC),通过消息鉴别码实现消息的源端鉴别和完整性检测,整个过程如图 3.34 所示。

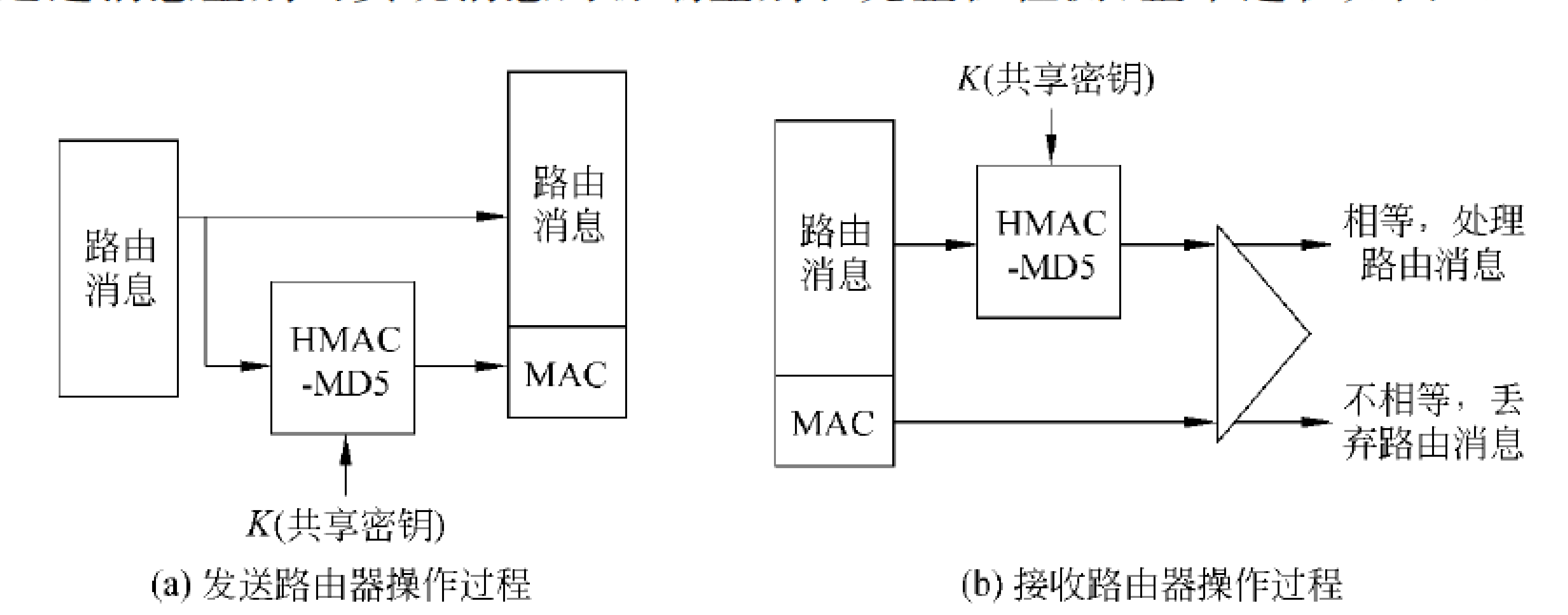


图 3.34 路由器和路由项鉴别过程

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 3.33 所示的网络结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图 3.35 所示。

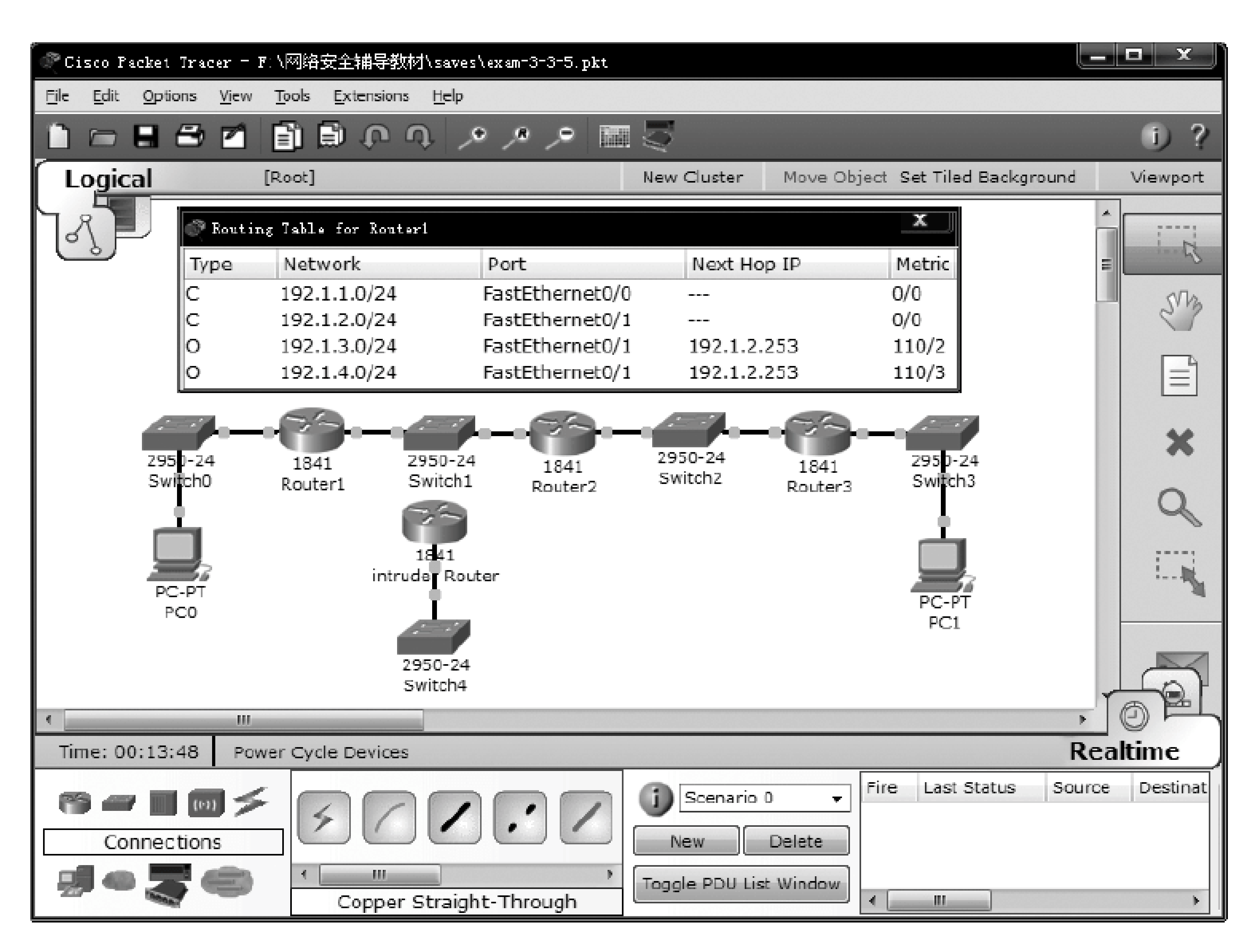


图 3.35 放置和连接设备后的逻辑工作区界面及 Router1 路由表

(2) 在路由器 Router1、Router2 和 Router3 上启动 OSPF 进程,指定参与区域 1 内动态路由项建立过程的接口,产生图 3.35 所示的 Router1 路由表。

(3) 接入 intruder Router,通过在接口 FastEthernet0/0 配置 IP 地址和子网掩码 192.1.4.254/24,假定 intruder Router 直接和网络 192.1.4.0/24 相连,启动 OSPF 进程,将接口 FastEthernet0/0 和 FastEthernet0/1 指定为参与区域 1 内动态路由项建立过程

的接口，产生图 3.36 所示错误的 Router1 路由表，目的网络 192.1.4.0/24 对应的下一跳改为 intruder Router。

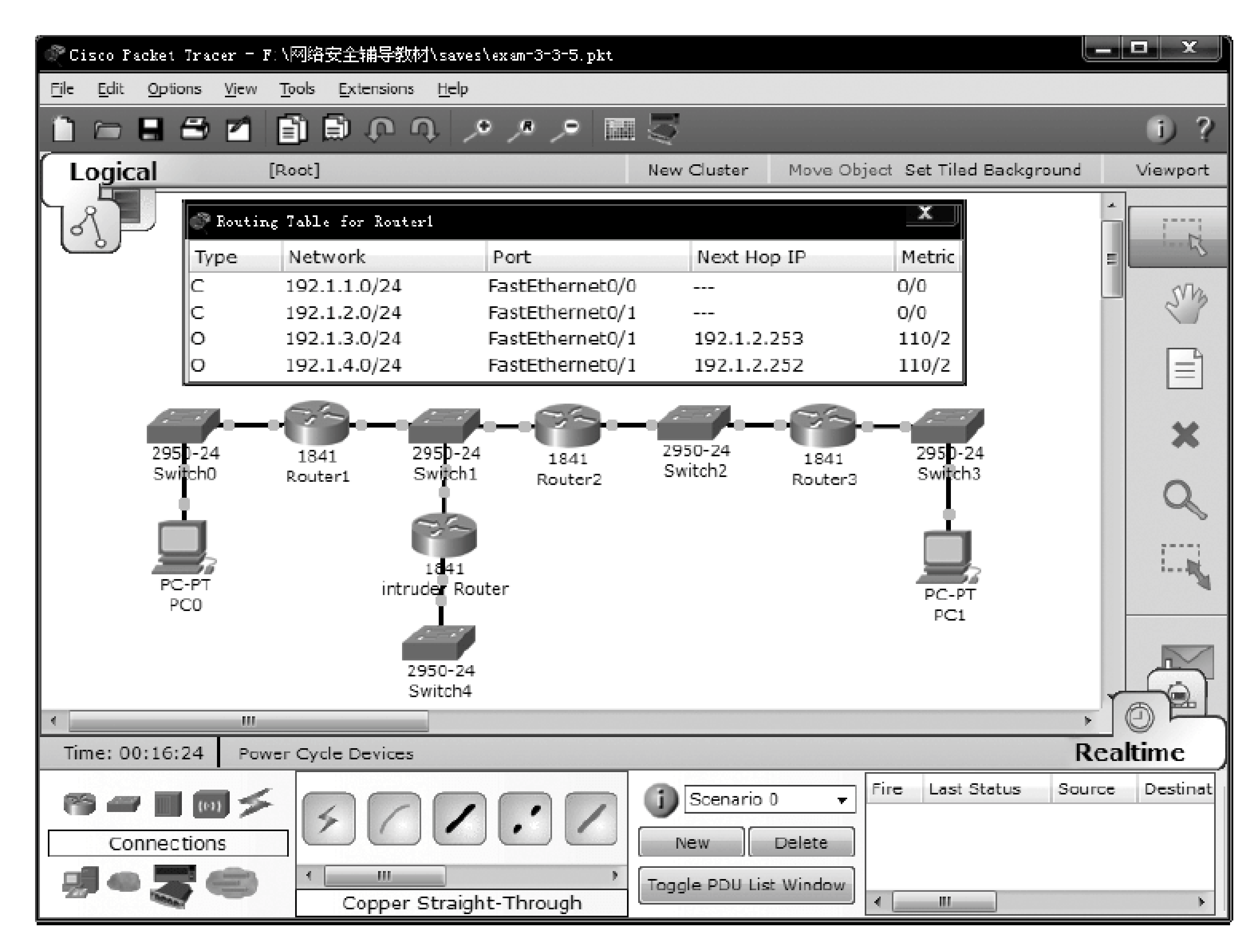


图 3.36　Router1 因 intruder Router 接入产生的错误路由表

(4) 在路由器 Router1、Router2 和 Router3 中启动区域 1 内路由消息源端鉴别和完整性检测机制，所有参与区域 1 内动态路由项建立过程的接口都需配置相同的消息鉴别码生成算法和密钥。由于每一个路由器只处理授权路由器发送、完整性检测准确且确定不是黑客截获后重放的链路状态信息和 Hello 报文，intruder Router 发送的链路状态信息和 Hello 报文不再影响区域 1 内动态路由项建立过程，Router1 路由表恢复正确内容，如图 3.37 所示。

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 11                    (启动 OSPF 进程，11 是进程标识符)
Router(config-router)#network 192.1.1.0 0.0.0.255 area 1
                         (通过 CIDR 地址块指定参与区域 1 动态路由项建立过程的接口，
```

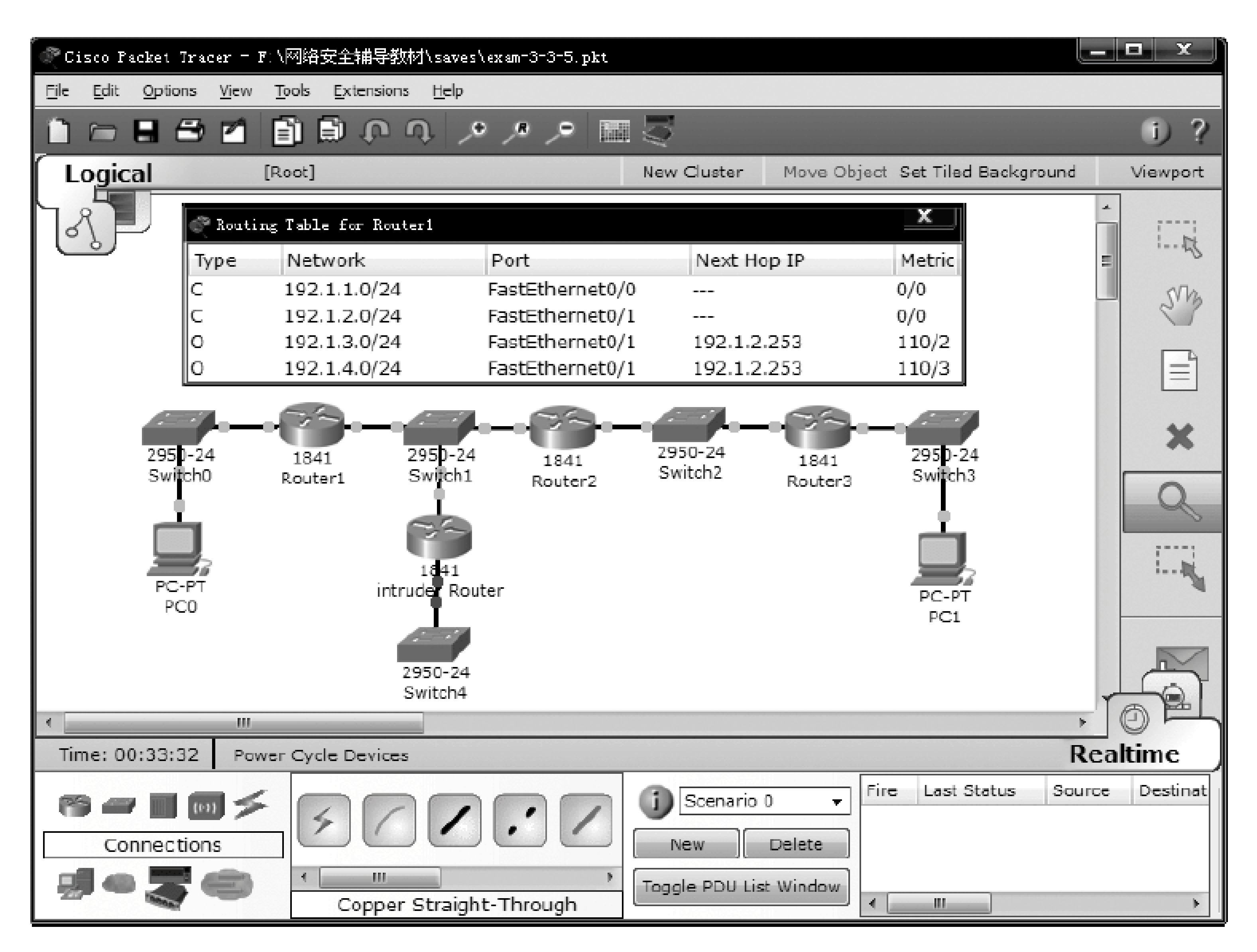


图 3.37 源端鉴别和完整性检测使得 intruder Router 不再对动态路由项建立过程产生影响

```
                                  接口 FastEthernet0/0 的接口地址属于 192.1.1.0/24)
Router(config-router)#network 192.1.2.0 0.0.0.255 area 1
                                  (通过 CIDR 地址块指定参与区域 1 动态路由项建立过程的接口，
                                  接口 FastEthernet0/1 的接口地址属于 192.1.2.0/24)
Router(config-router)#exit
```

以下是和鉴别相关的配置。

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip ospf authentication message-digest    (用 HMAC 产生消息鉴别码)
Router(config-if)#ip ospf message-digest-key 1 md5 abcd
                                  (报文摘要算法采用 MD5,密钥编号为 1,密钥为 abcd)
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 abcd
Router(config-if)#exit
Router(config)#router ospf 11
Router(config-router)#area 1 authentication message-digest
                                  (区域 1 内链路状态信息采用消息鉴别码进行源端鉴别和完整性检测)
Router(config-router)#exit
```

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
```

```
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.253 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.254 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 12
Router(config-router)#network 192.1.2.0 0.0.0.255 area 1
Router(config-router)#network 192.1.3.0 0.0.0.255 area 1
Router(config-router)#exit
```

以下是和鉴别相关的配置。

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 abcd
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 abcd
Router(config-if)#exit
Router(config)#router ospf 12
Router(config-router)#area 1 authentication message-digest
Router(config-router)#exit
```

(3) Intruder Router 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.252 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 14
Router(config-router)#network 192.1.2.0 0.0.0.255 area 1
Router(config-router)#network 192.1.4.0 0.0.0.255 area 1
Router(config-router)#exit
```

Router3 命令行配置过程与 Router1 和 Router2 命令行配置过程相似,不再赘述。

3.3.6 审计实验

1. 实验内容

(1) 完成网络配置。

(2) 完成和审计有关的配置。

(3) 检查日志服务器记录的信息。

2. 网络结构

网络结构如图 3.38 所示。通过配置路由器,可以将发生在路由器上的事件记录到日志服务器,通过分析日志服务器记录的事件,能够发现网络可能遭受的黑客攻击。日志服务器记录的事件种类通过配置确定,这里要求路由器将每一次远程配置过程记录到日志服务器,无论该次远程配置过程是否成功。

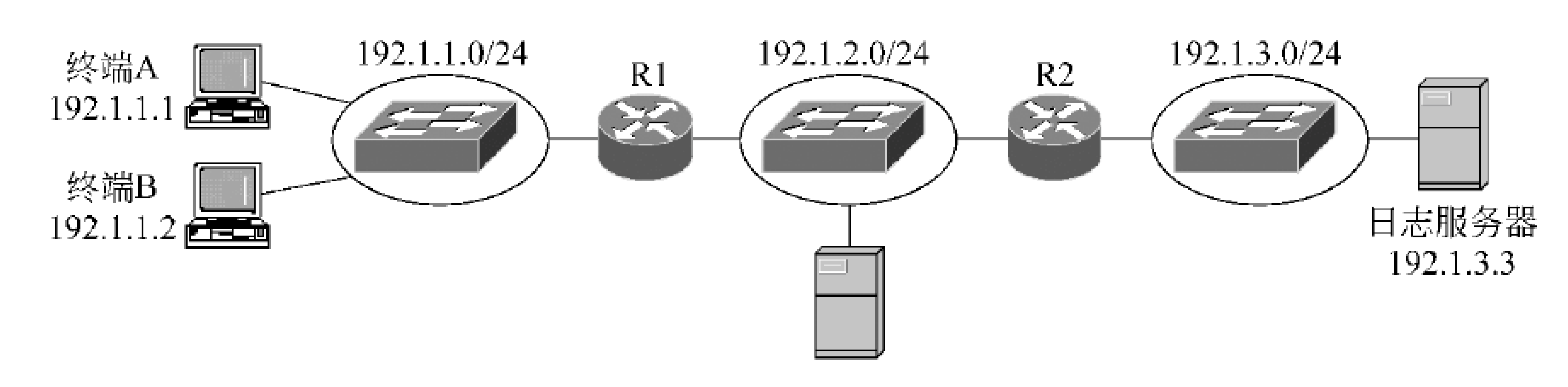


图 3.38 网络结构

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 3.38 所示的网络结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图 3.39 所示。

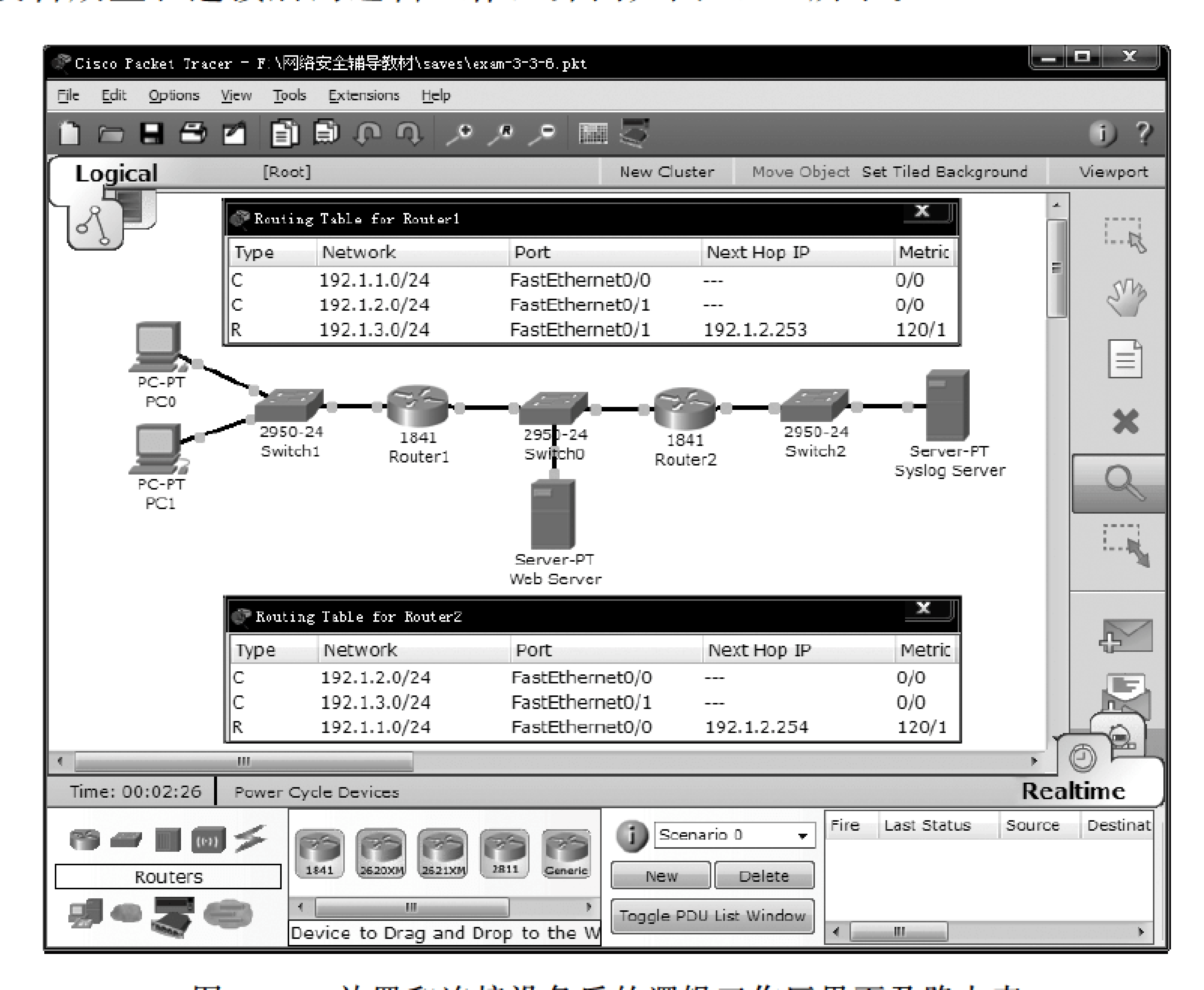


图 3.39 放置和连接设备后的逻辑工作区界面及路由表

(2) 完成路由器接口 IP 地址和子网掩码配置,通过配置 RIP,每一个路由器建立到达与其没有直接连接的网络的传输路径。路由器建立的完整路由表如图 3.39 所示。

(3) 开放两个路由器的远程配置功能,在每一个路由器的本地用户库设置用于远程登录路由器的用户名和口令。

(4) 配置日志服务器地址,开启向日志服务器发送用于记录事件的消息的功能,将远程登录设备成功和失败定义为需要记录的事件。这样,终端每一次远程配置路由器过程都被记录到日志服务器,无论该次远程配置过程成功与否。

(5) 在 PC1 上开始远程登录 Router2 过程,输入错误的用户名和口令,导致本次远程登录失败,如图 3.40 所示。日志服务器记录下该次失败的远程登录过程,如图 3.42 所示。图中 HostName 字段给出路由器发送消息的接口的 IP 地址。

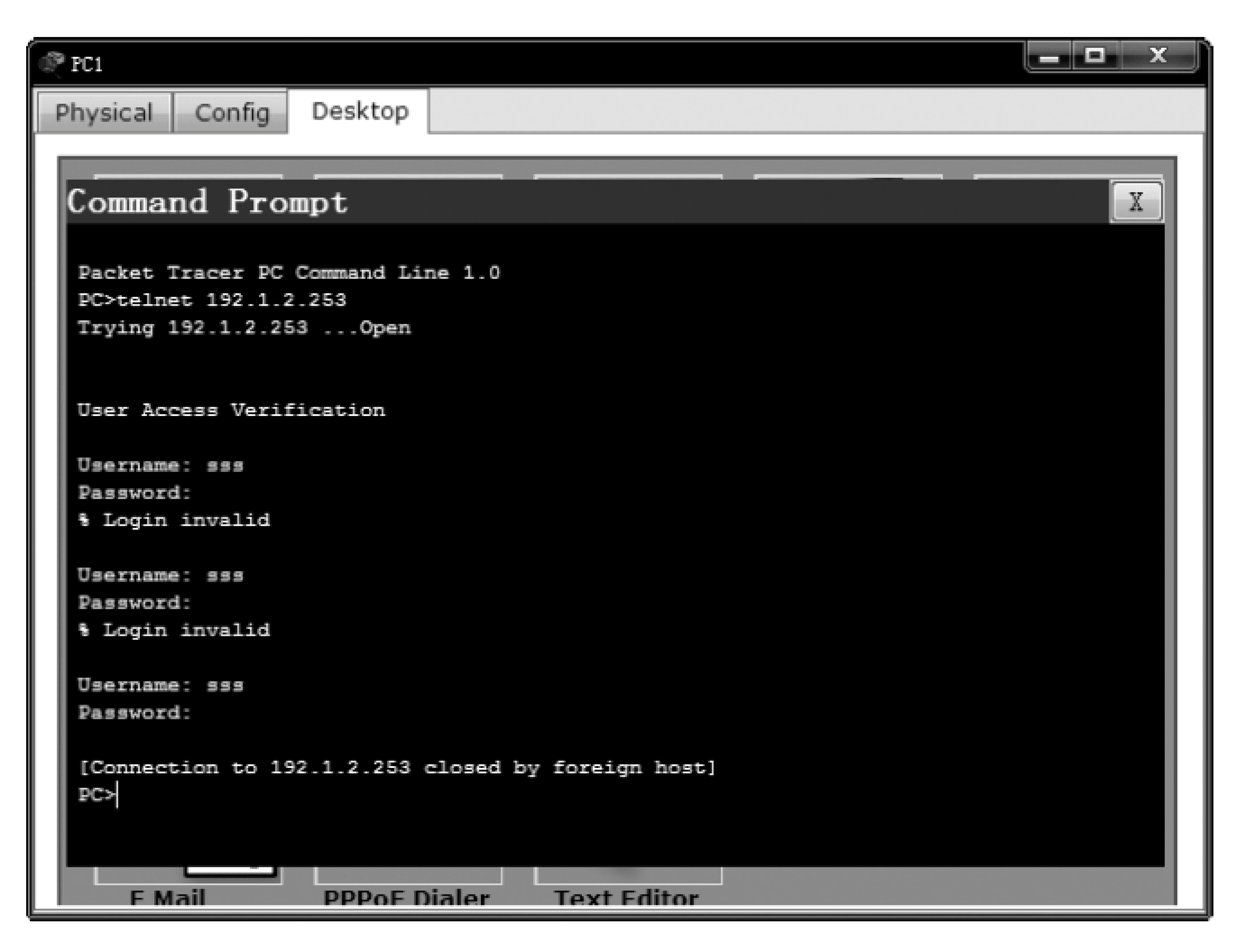


图 3.40　远程配置 Router2 失败界面

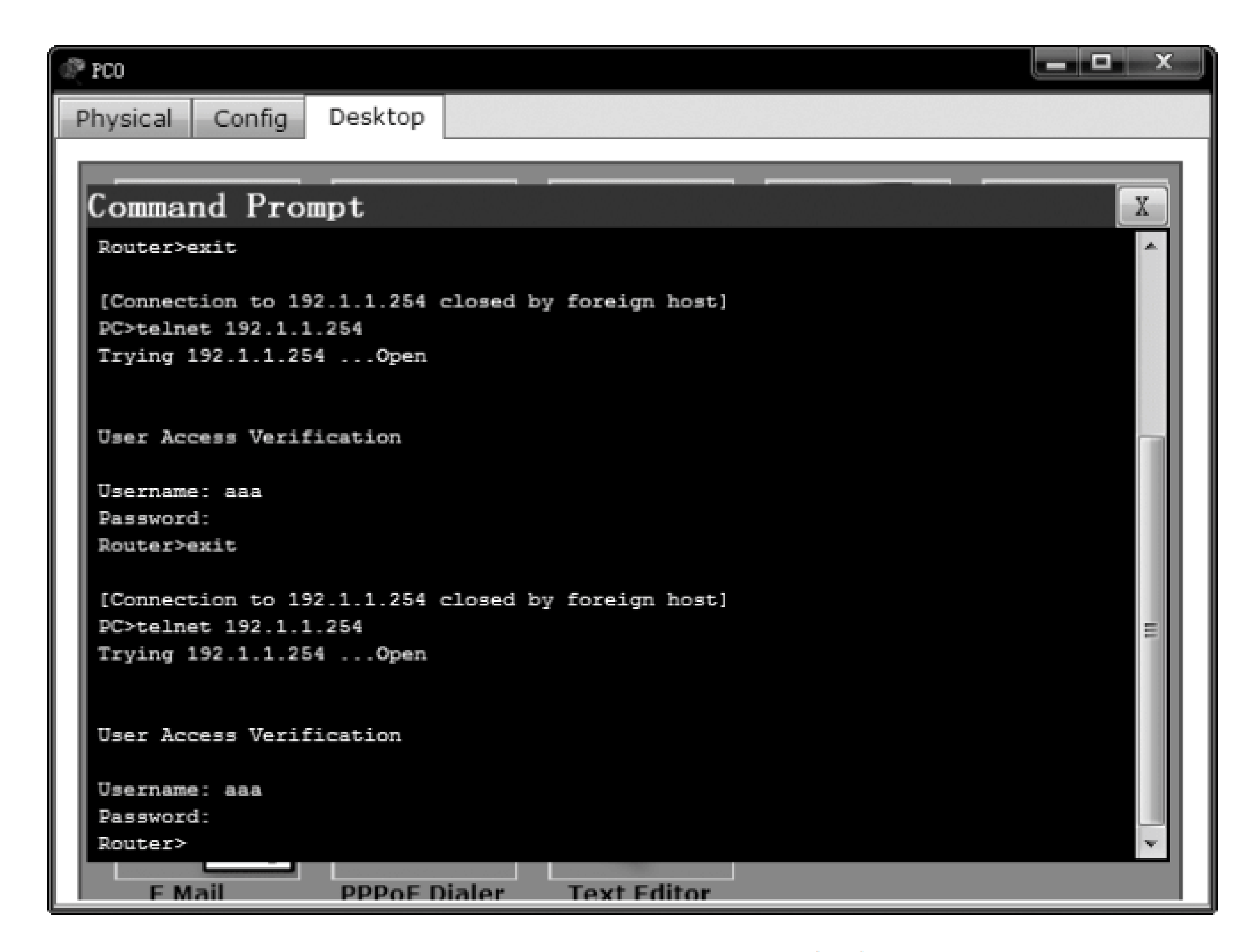


图 3.41　远程配置 Router1 成功界面

(6) 在 PC0 上开始远程登录 Router1 过程，输入正确的用户名和口令，实现成功登录，如图 3.41 所示。日志服务器记录下该次成功的远程登录过程，如图 3.42 所示。

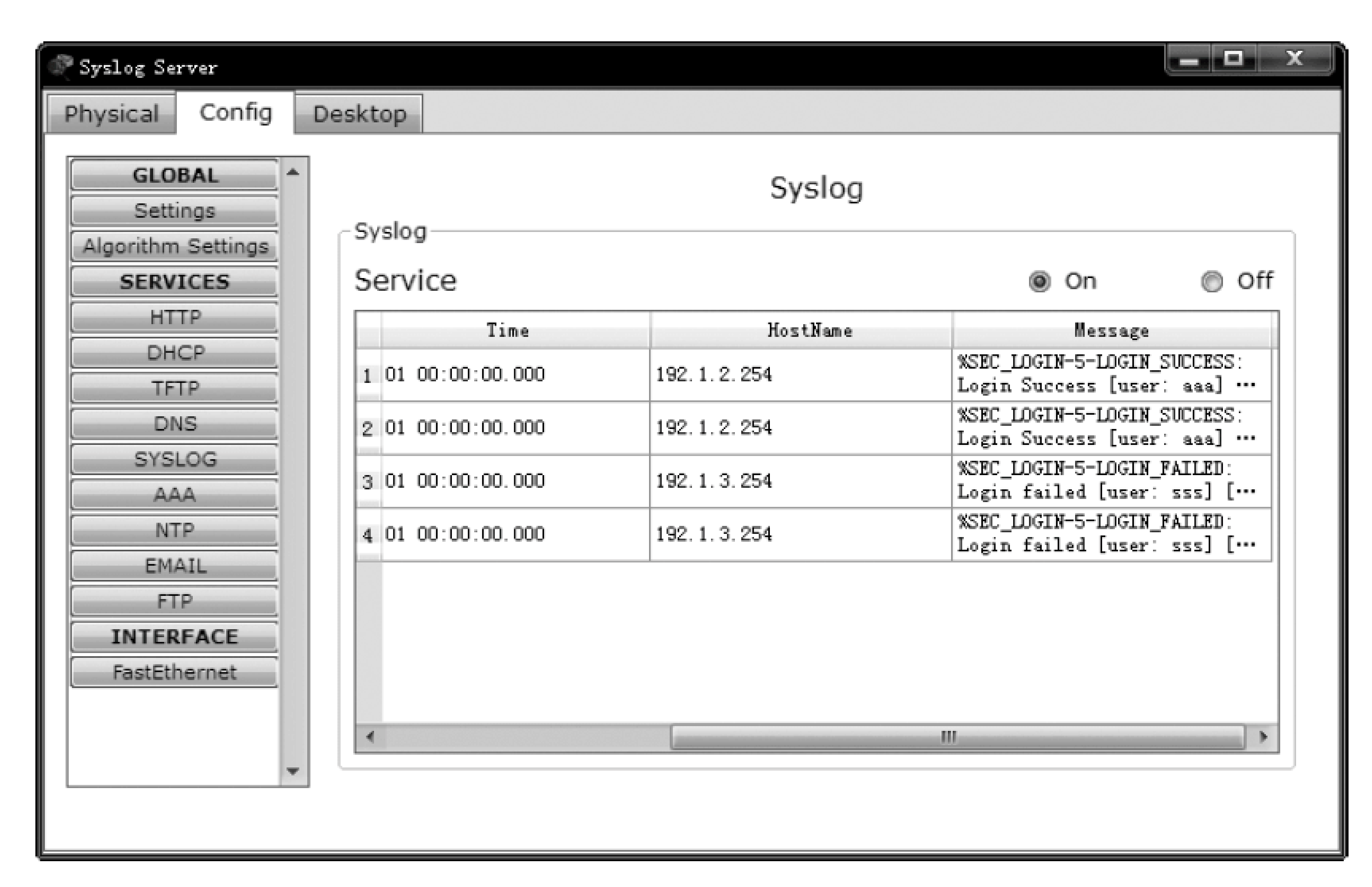


图 3.42　日志服务器记录的路由器远程配置过程

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#username aaa password bbb
                                        (在本地用户库配置用于远程登录路由器的用户名和口令)
Router(config)#line vty 0 15                (进入虚拟终端配置模式)
Router(config-line)#login local           (用本地用户库定义的用户名和口令验证远程登录用户)
Router(config-line)#exit
Router(config)#enable password aaa        (配置进入全局配置模式的口令)
Router(config)#logging host 192.1.3.3     (配置日志服务器 IP 地址)
Router(config)#logging on                 (开启记录事件功能)
Router(config)#login on-success log       (日志服务器记录下每一次成功的远程登录过程)
Router(config)#login on-failure log       (日志服务器记录下每一次失败的远程登录过程)
```

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#username ccc password ddd
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
```

```
Router(config)#enable password ccc
Router(config)#logging host 192.1.3.3
Router(config)#logging on
Router(config)#login on-failure log
Router(config)#login on-success log
```

第4章 加密和报文摘要算法

CHAPTER

4.1 知识要点

4.1.1 加密算法分类

1. 加密解密本质

加密是对数据的一种数学变换，解密是一种和加密互逆的数学变换。将原始数据称为明文，将明文数学变换后的结果称为密文。对明文进行的数学变换称为加密，对密文进行的数学变换称为解密，对密文进行数学变换将重新还原出明文。加密和解密过程需要密钥参与，参与加密过程的密钥称为加密密钥，参与解密过程的密钥称为解密密钥，数据加密传输过程如图4.1所示。

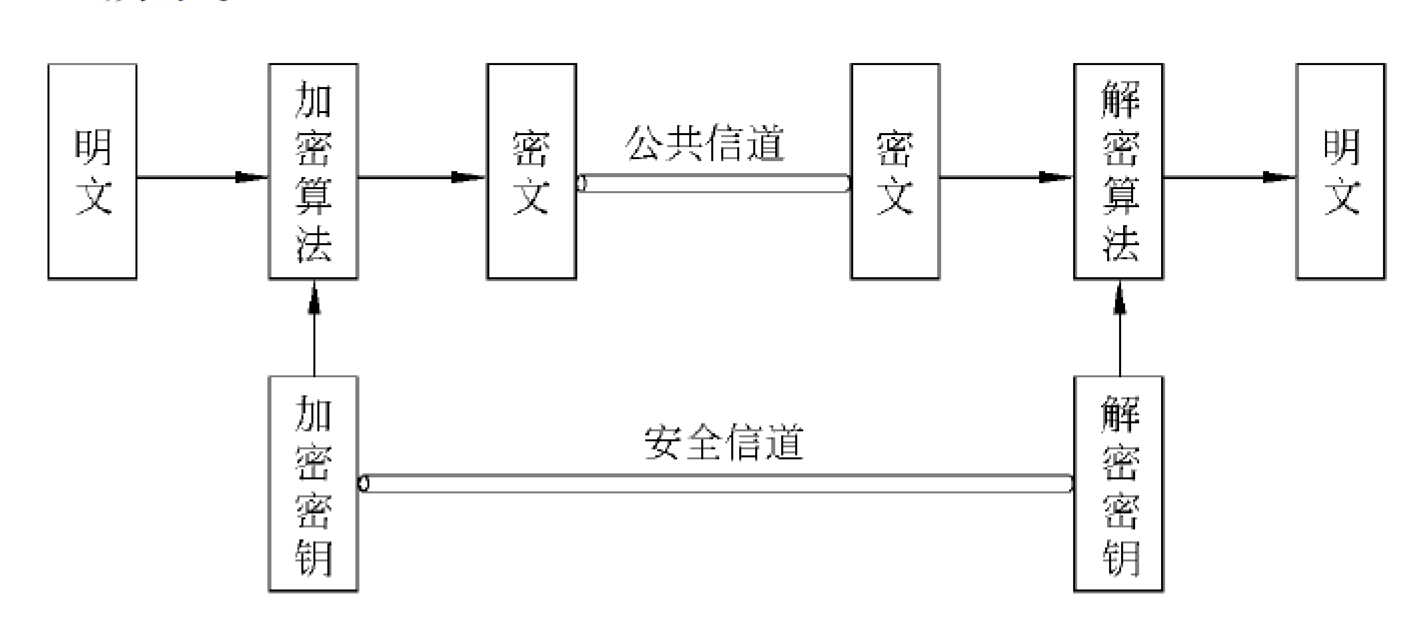


图4.1 数据加密传输过程

2. 密钥的含义

密钥是完成数学变换需要用到的参数。假定加密算法为 $Y=aX+b$，其中 X 是明文，Y 是密文，则参数 a 和 b 就是密钥，相同明文，不同密钥，得出不同的密文。知道加密算法，如果不知道密钥，也无法根据明文计算出密文。

3. 对称密钥算法和不对称密钥算法

如果某种加密算法的加密密钥和解密密钥相同，或者可以通过其中一个密钥推导出另一个密钥，称这种加密算法为对称密钥算法。如果某种加

密算法的加密密钥和解密密钥不同，且根据现有计算能力无法根据其中一个密钥推导出另一个密钥，称这种加密算法为不对称密钥算法。

现代密码体制要求公开加密解密算法，因此密文的安全性完全取决于密钥。对称密钥算法由于需要在发送端和接收端同步密钥，因此存在密钥分发问题，即密钥必须在进行数据加密传输过程前分发到所有参与数据加密传输过程的终端。实现密钥的安全分发有一定的难度，但一旦泄漏密钥，加密传输的安全性便荡然无存。

4. 加密算法的安全性

加密算法的安全性取决于解析出密钥的难度，好的加密算法即使获得有限的明文、密文对，也无法解析出密钥。对于加密算法 $Y=aX+b$，只要获得两对明文、密文对（X，Y），就可通过二元一次方程解析过程求出密钥 a 和 b，因此加密算法 $Y=aX+b$ 不是一种有用的加密算法。

安全的加密算法必须保证：除了穷举法外，不存在其他更有效的解析密钥的方法。穷举法解析密钥的难度取决于密钥的长度，如果密钥的长度为 N 位二进制数，则可能存在 2^N 个密钥，通过穷举法解析出密钥的平均尝试次数为 $2^N/2$。

5. 对称密钥算法

对称密钥算法包含分组密码和流密码。

（1）分组密码

分组密码将需要加密的明文分为长度固定的数据段，然后对每一段数据段进行加密，得到等长的密文。分组密码加密运算过程的安全性取决于以下几个因素。

- 数据段长度：增加数据段的长度，有利于提高加密算法的安全性（不容易通过明文、密文对解析出密钥），但增加了运算复杂性。
- 密钥长度：增加密钥长度，增加密钥空间，使得穷举法攻击变得不可行。
- 加密算法：采用复杂的加密算法，使得穷举法成为唯一的有效破译手段。目前通过多级替代和置换运算实现数据变换。

（2）流密码

流密码，又称为序列密码，是一次一密钥的加密运算过程，发送端在密钥集中随机产生一个与明文 P 相同长度的密钥 K，密钥 K 和明文 P 进行异或运算后得到密文 Y。接收端用同样的密钥 K 和密文 Y 进行异或运算，还原出明文 P。如果密钥集足够大，每一次加密运算的密钥不同，且这些密钥之间不存在相关性，这种密码体制是最安全的。

6. 不对称密钥算法

不对称密钥算法，也称为公开密钥加密算法，使用不同的加密密钥和解密密钥，发送端用加密算法 E 和密钥 PK 对明文 P 进行加密，接收端用解密算法 D 和密钥 SK 对密文 Y 进行解密。加密密钥 PK 是公开的，而解密密钥 SK 是保密的，只有接收端知道，用于解密用公开密钥加密的密文。习惯上将加密密钥称为公钥，而将解密密钥称为私钥。

$$Y = E_{\mathrm{PK}}(P)$$

$$D_{\mathrm{SK}}(Y) = D_{\mathrm{SK}}(E_{\mathrm{PK}}(P)) = P$$

公开密钥加密算法的原则如下。

- 容易成对生成密钥 PK 和 SK。
- 加密和解密算法是公开的，而且可以对调，$D_{SK}(E_{PK}(P))=E_{PK}(D_{SK}(P))=P$。
- 加密和解密过程容易实现。
- 从计算可行性讲，无法根据 PK 推导出 SK。
- 从计算可行性讲，无法根据 PK 和密文 Y 推导出明文 P。

同样，公开密钥加密算法的私钥长度也必须足够长，这样才能有效防御穷举法攻击。但公开密钥加密算法的计算复杂性和密钥长度之间不是线性关系，增加密钥长度会急剧增加计算复杂性，因此，一般不会直接用公开密钥加密算法加密需要传输的数据。

7. 数字信封

对称密钥加密算法的优势是加密解密运算过程相对简单，计算量相对较少，劣势是密钥的分发比较困难。公开密钥加密算法的劣势是加密解密运算过程比较复杂，计算量相对较大，因此不适合大量数据加密的应用环境。优势是密钥分发简单，可以通过有公信力的传播媒介公告公钥。

图 4.2 是这两种密钥体制完美结合的应用实例，假定发送端拥有接收端的公钥 PKA，当发送端需要加密发送给接收端的数据时，发送端随机产生密钥 K，用密钥 K 和对称密钥加密算法如 DES，加密发送给接收端的数据，产生数据密文 Y1（$Y1=DESE_K$（数据）），同时，用接收端的公钥 PKA 和 RSA 加密算法加密对称密钥 K，产生密钥密文 Y2（$Y2=RSAE_{PKA}(K)$），将数据密文 Y1 和密钥密文 Y2 串接在一起发送给接收端。接收端用公钥 PKA 对应的私钥 SKA 和 RSA 解密算法解密出密钥 K（$RSAD_{SKA}(RSAE_{PKA}(K))=K$），然后用密钥 K 和对称密钥解密算法解密出数据（$DESD_K(DESE_K$（数据））＝数据）。这里 DESE 表示 DES 加密算法，DESD 表示 DES 解密算法，RSAE 表示 RSA 加密算法，RSAD 表示 RSA 解密算法。用公开密钥算法和公钥加密对称密钥产生的密钥密文称为数字信封。

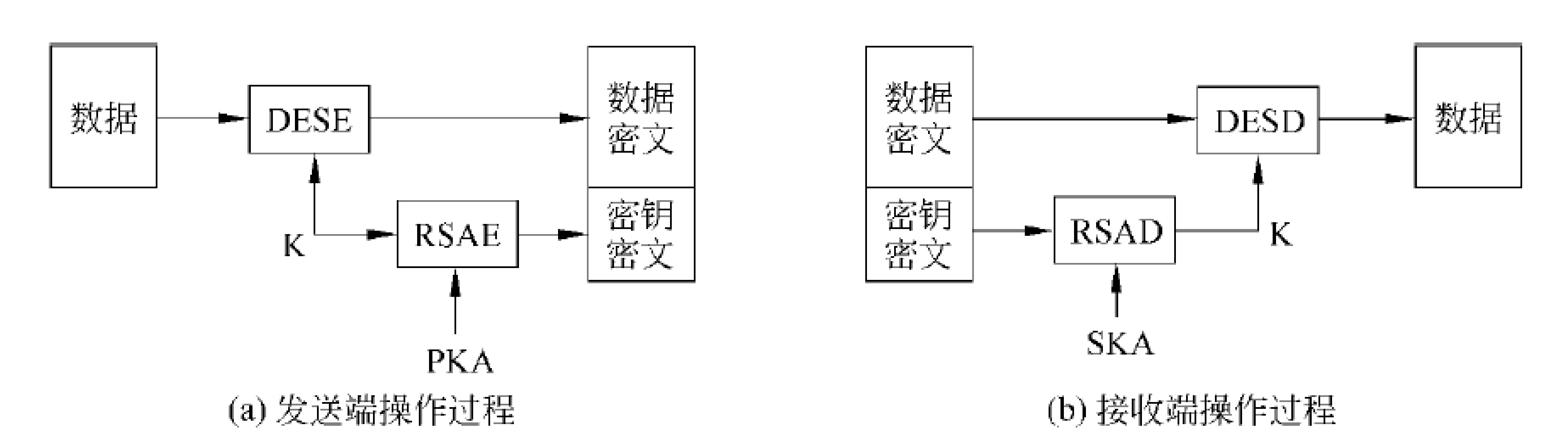


图 4.2　两种密钥体制完美结合的应用实例

4.1.2　报文摘要算法的单向性和抗冲突性要求

报文摘要算法的目的就是产生用来标识某个任意长度报文的有限位数信息，即报文摘要，而且这种标识信息就像报文的指纹一样，具有确认性和唯一性。假定 MD 为报文摘要算法，MD(X)是报文摘要算法对报文 X 作用后产生的标识信息，MD 必须满足如下要求。

- 能够作用于任意长度的报文。

- 产生有限位数的标识信息。
- 易于实现。
- 具有单向性，即只能根据报文 X 求出 MD(X)。从计算可行性讲，无法根据标识信息 h 得出报文 X，且使得 MD(X)＝h。
- 具有抗冲突性。从计算可行性讲，对于任何报文 X，无法找出另一个报文 Y，$X \neq Y$，但 MD(X)＝MD(Y)。
- 即使只改变报文 X 中一位二进制位，也使得重新计算后的 MD(X)变化很大。

4.1.3 加密和报文摘要算法在网络安全中的作用

数据经过计算机网络传输，除了需要通过加密来保证数据的保密性外，还需要确定数据传输过程中是否被黑客恶意篡改，需要验证数据发送端的身份，需要防止某个发送端抵赖曾经发送过的数据。

1. 加密

存储和发送数据时对数据加密，读取和接收数据时对数据解密，如果 P 为明文，Y 为密文，E 为加密算法，D 为解密算法，Ke 为加密密钥，Kd 为解密密钥，则 $Y=E_{\mathrm{Ke}}(\mathrm{P})$，$P=D_{\mathrm{Kd}}(Y)$。通常情况下，$D_{\mathrm{Kd}}(E_{\mathrm{Ke}}(P))=E_{\mathrm{Ke}}(D_{\mathrm{Kd}}(P))=P$。

2. 完整性检测

为了检测出消息 P 传输过程中所有可能发生的恶意篡改，发送端将对根据消息 P 计算出的报文摘要进行加密，并将加密后的报文摘要附在消息 P 后一起发送给接收端。接收端接收到消息 P 和附在消息 P 后面加密后的报文摘要后，先对加密的报文摘要解密，还原出发送端计算出的报文摘要，然后对消息 P 进行报文摘要运算，并将计算结果和解密后的报文摘要进行比较，如果相等，表示消息 P 在传输过程中未被篡改；如果不相等，则表示消息 P 已经被篡改。整个过程如图 4.3 所示。

[redacted]术检测消息完整性的过程

报文摘要作为消息完整性检测机制，必须使发送端和接收端拥有共同密钥 K，且所有可能的篡改者无法获得密钥 K，同时报文摘要算法保证，对于消息 P，根据现有计算能力，篡改者无法得出消息 P'，$P \neq P'$，但 MD(P)＝MD(P')。这样篡改者无法做到既篡改消息 P，又不让接收端检测出消息 P 已经被篡改。

如果密钥 K 只有发送端和接收端知道，则图 4.3 所示的完整性检测过程也是源端鉴别过程。

3. 身份鉴别

身份鉴别与源端鉴别有所不同，源端鉴别是接收端验证数据的发送端的过程，身份鉴别是由服务器验证某个用户宣示的身份和其真实身份是否一致的过程。当用户请求服务器提供只对授权用户提供的服务时，服务器只有在通过身份鉴别确定该用户是授权用户的情况下，才能响应该用户的服务请求。服务器鉴别某个用户身份前必须拥有该用户的鉴别信息，且保证该用户的鉴别信息只有服务器和该用户知道。身份鉴别过程就是用户

向服务器提供鉴别信息的过程，但需要保证用户向服务器提供鉴别信息的过程不会导致鉴别信息外泄。

图4.4是单向鉴别身份过程。口令PASSA只有用户A和服务器知道，服务器只要确认某个用户知道口令PASSA，就可断定该用户是用户A，用户A需要采用保密传输方式向服务器传输口令PASSA。服务器首先向用户传输一个随机数C，由于该随机数是从一个很大的数字空间产生的，在较长一段时间内不会产生相同的随机数。用户终端接收到随机数后，将随机数C和口令串接在一起，对串接结果进行MD5运算，将用户名和MD5运算结果传输给服务器。服务器同样将随机数C和用户A对应的口令串接在一起，对串接结果进行MD5运算，如果运算结果和用户终端发送的MD5运算结果相同，用户A身份得到确认。由于报文摘要算法的单向性，即使黑客截获报文摘要运算结果，也无法得到口令PASSA。服务器首先发送随机数的目的是防止黑客通过预先截获的用户A发送给服务器的鉴别信息，冒充用户A通过服务器的身份鉴别。

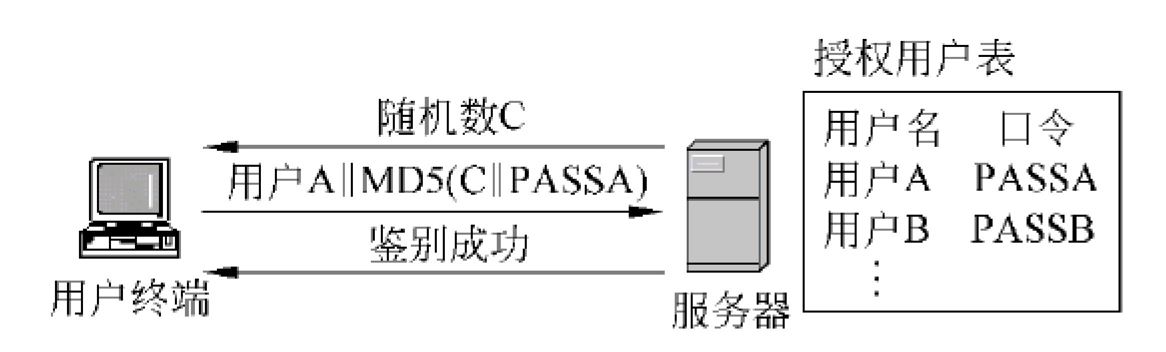


图4.4　单向身份鉴别过程

身份鉴别和源端鉴别之间存在关联，通常在身份鉴别过程中将某个用户和某种标识信息绑定在一起，然后在数据传输过程中，通过检测数据报文中是否携带该标识信息来验证数据的发送端。802.1X用MAC地址作为和用户绑定的标识信息，Internet接入用连接用户终端的信道和IP地址作为和用户绑定的标识信息。如果身份鉴别过程用共享密钥K作为某个发送端的标识信息（即只有发送端和接收端知道共享密钥K），可用图4.3所示的源端鉴别过程鉴别发送端身份。

4. 数字签名

数字签名必须保证唯一性、关联性和可证明性。唯一性保证只有特定发送端能生成数字签名，关联性保证是对特定报文的数字签名，可证明性表明该数字签名的唯一性和与特定报文的关联性可以得到证明。

公开密钥算法中公钥和私钥一一对应，私钥具有私密性，只有用户本身知道，如果公钥和用户之间的绑定关系能够被权威机构证明，具有不可否认性。数字签名实现过程如图4.5所示。用户A用私钥SKA对明文P经过报文摘要运算后得到的摘要MD(P)进行解密运算，产生数字签名(D_{SKA}(MD(P)))，将明文P和数字签名一同发送给用户B。用户B认定明文P是用户A发送的前提是：用与用户A绑定的公钥PKA对数字签名进行加密运算后得到的结果和对明文P进行报文摘要运算后得到的结果相同，即E_{PKA}(数字签名)=MD(P)。D_{SKA}(MD(P))能够作为发送端用户A对报文P的数字签名的依据如下：一是私钥SKA只有用户A知道，因此只有用户A才能实现D_{SKA}(MD(P))运算过程，保证了数字签名的唯一性；二是根据报文摘要算法的特性，即从计算可行性讲，其他用户无法生成某个报文P'，$P\neq P'$，但MD(P)=MD(P')，因此MD(P)只能是针对

报文 P 的报文摘要算法的计算结果，保证了数字签名和报文 P 之间的关联性；三是数字签名能够被核实，因为公钥 PKA 和私钥 SKA 一一对应，如果公钥 PKA 和用户 A 之间的绑定关系得到权威机构证明，一旦证明用公钥 PKA 对数字签名进行加密运算后还原的结果（E_{PKA}（数字签名））等于报文 P 的报文摘要（MD（P）），就可证明数字签名是 D_{SKA}（MD（P））。

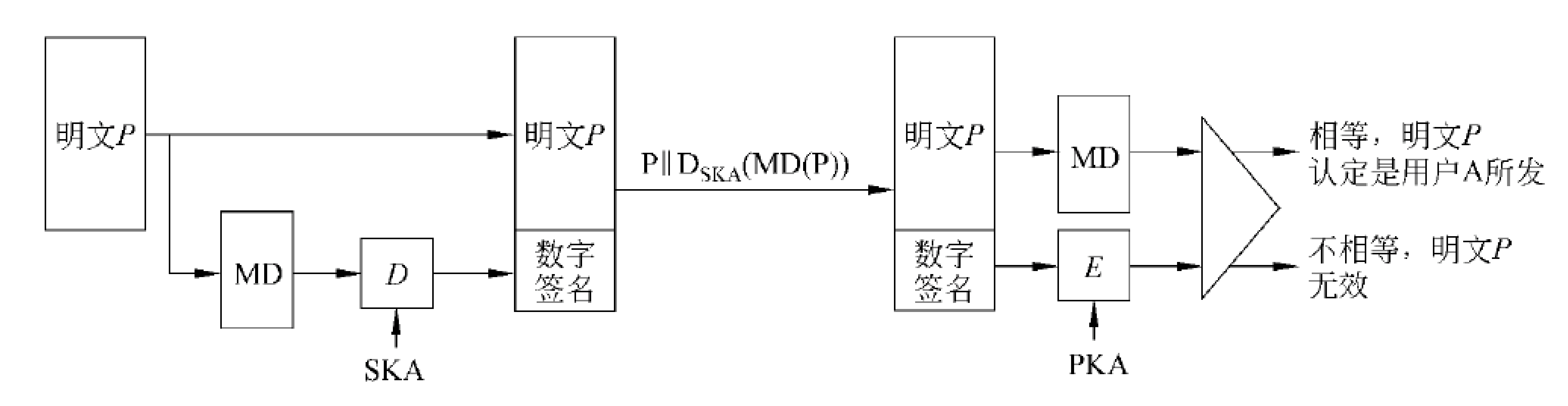


图 4.5 数字签名实现过程

用公开密钥算法实现数字签名的前提是：由权威机构出具证明用户和公钥之间绑定关系的证书，只有公钥和用户之间的绑定关系得到有公信力的权威机构的证实，才能核定该用户的数字签名。

4.2 例题解析

4.2.1 自测题

1. 选择题

（1）现代密码体制用下述________保证密文安全性。

A. 保密加密算法　B. 保密解密算法　C. 保密加密密钥　D. 保密解密密钥

（2）好的加密算法只能采用下述________方法破译密文。

A. 穷举　B. 数学分析　C. 明文和密文对照　D. 分析密文规律

（3）加密算法安全性受到下述________挑战。

A. 网格计算　B. 高速计算机　C. 人工分析　D. 数学分析

（4）安全的加密算法具有下述________特点。

A. 只能用穷举法破译密文　B. 密钥长度足够

C. 经得住网格计算考验　D. 以上全部

（5）安全的加密算法满足下述________条件。

A. 无法破译密文

B. 破译密文的成本超过密文信息价值

C. 破译密文时间超过密文有效期

D. B 或 C

（6）网络安全中，加密算法的用途包含下述________。

A. 加密信息　B. 信息完整性检测　C. 用户身份鉴别　D. 以上全部

（7）下述________不是报文摘要算法的特点。
A. 固定长度报文摘要　　B. 单向性
C. 抗冲突性　　D. 算法难以实现

（8）下述________不是分组密码的特点。
A. 明文分成固定长度数据段　　B. 加密运算由多次替代和置换构成
C. 和明文数据段等长的密文　　D. 不同长度的加密和解密密钥

（9）下述________不是 RSA 加密算法的特点。
A. 公钥和私钥不同
B. 无法根据公钥推导出私钥
C. 密文和明文等长
D. 可靠性基于大数因子分解困难的事实

（10）下述________是用 RSA 生成数字签名的先决条件。
A. 公钥和私钥一一对应
B. 私钥只有签名者自己知道
C. 由权威机构证明公钥和签名者之间关联
D. 以上全部

（11）数字签名中对报文进行报文摘要运算是确定数字签名与报文之间的________。
A. 关联性　　B. 保密性　　C. 可证明性　　D. 以上全部

（12）下述________算法属于对称密钥算法。
A. RSA　　B. MD5
C. Diffie-Hellman 密钥交换算法　　D. 流密码

（13）下述________算法属于不对称密钥算法。
A. RSA　　B. MD5　　C. DES　　D. AES

（14）下述________不属于不对称密钥算法的优点。
A. 公钥和私钥不同　　B. 公钥可以公开
C. 适合实现数字签名　　D. 计算复杂性大

（15）下述________属于对称密钥算法的优点。
A. 加密密钥和解密密钥相同　　B. 计算复杂性小
C. 多对一加密通信需要多个密钥　　D. 接收端能够修改密文

（16）下述________不属于流密码的特点。
A. 一次一密　　B. 从很大密钥空间中随机产生密钥
C. 密钥之间没有关联性　　D. 加密密钥和解密密钥相同

2. 填空题

（1）加密算法根据加密密钥和解密密钥是否相同可以分为________和________，其中分组密码和流密码属于________，RSA 属于________。

（2）分组密码的特点包括________、________和________，目前常见的分组密码有________和________。

（3）分组密码的安全性取决于________、________和________。RSA 的安全性取决

于________,但 RSA 增加________,会急剧增加加密解密运算的复杂性。

(4) 报文摘要算法的特点包括________、________、________和________。它在网络安全中的用途包括________、________和________。

(5) 不对称密钥算法的特点包括________、________、________和________。它在网络安全中的用途包括________、________和________。

(6) 对称密钥算法的主要缺点包括________、________和________。

(7) 消息鉴别码的作用是________和________,它通常是________。

3. 名词解释

____数字信封 ____密钥

____对称密钥算法 ____不对称密钥算法

____ AES ____穷举

____分组密码 ____流密码

____报文摘要算法 ____ MD5

____ SHA-1 ____ HMAC

____数字签名 ____身份鉴别

____加密 ____解密

____ RSA ____ DES

____完整性检测 ____源端鉴别

(a) 加密密钥和解密密钥相同,或者可以通过一个密钥推导出另一个密钥的加密解密算法。

(b) 加密密钥和解密密钥不同,且无法通过一个密钥推导出另一个密钥的加密解密算法。

(c) 一种属于对称密钥算法,将明文分成长度固定的数据段,每一段数据段单独进行加密运算,产生和数据段等长的密文的加密算法。

(d) 一种属于对称密钥算法,采用一次一密,用和明文等长的密钥和明文异或操作产生密文的加密算法。

(e) 一种可靠性基于大数因子分解困难的事实的不对称加密算法。

(f) 数据加密标准,一种将明文分为 64 位长度的数据段,用 56 位密钥(加上 8 位奇偶校验位后为 64 位)对每一段数据段加密运算,产生 64 位密文的分组密码加密算法。

(g) 高级加密标准,一种将明文分为最小长度为 128 位的数据段,用最小长度为 128 位的密钥对每一段数据段加密运算,产生和明文数据段等长密文的分组密码加密算法。

(h) 在获取多对明文、密文对的情况下,只有通过尝试密钥空间中的每一个密钥才能确定用于解密密文的密钥的破译密文方法。

(i) 一种将任意长度报文映射到固定长度摘要,并使这种映射具有单向性和抗冲突性的算法。

(j) 报文摘要第 5 版,一种把任意长度报文映射为 128 位长度摘要的报文摘要算法。

(k) 安全散列算法第 1 版,一种把任意长度报文映射为 160 位长度摘要的报文摘要算法。

(l) 散列消息鉴别码,一种将密钥和报文的串接结果通过报文摘要算法映射为固定长度的消息鉴别码的算法。

(m) 一种将明文转换成密文的数学变换。

(n) 一种将密文还原成明文的数学变换。

(o) 一种通过在报文后附加消息鉴别码,检测出报文在传输过程中发生的任何改变的技术。

(p) 一种通过在报文中嵌入发送端标识信息,使得接收端能够验证报文发送端的技术。

(q) 一种具有唯一性、与特定报文关联性,且其唯一性和与特定报文关联性可以被第三方证明的消息鉴别码,发送端一旦在报文后附加这种消息鉴别码,将无法抵赖曾经发送过该报文的事实。

(r) 某个用户通过向鉴别者提供只有其和鉴别者知道的用户标识信息来证明自己身份的过程。

(s) 一种为实现发送端和接收端之间对称密钥安全传输,用公开密钥算法和公钥加密对称密钥产生的密钥密文。

(t) 一种参与加密解密运算过程的参数,在加密解密算法公开的情况下,该参数的安全性直接决定密文的安全性。

4. 判断题

(1) 目前存在的几种对称密钥加密算法,密文和明文等长。

(2) 穷举法破译密钥的难度与密钥空间大小成正比。

(3) 加密算法足够复杂的目的是避免通过数学分析的方法根据有限的明文、密文对解析出密钥。

(4) 存在永远无法破译的密文。

(5) 安全的加密算法要求破译密文所需时间足够长,或者破译密文所付出的代价足够大。

(6) 加密算法在网络安全中的作用仅仅是加密传输的数据。

(7) 为了安全起见,对称密钥加密算法一般采用一次一密。

(8) 同一密钥,加密数据的次数越多,破译的可能性越大。

(9) 同一密钥,使用的时间越长,破译的可能性越大。

(10) 不存在摘要相同的两个不同报文。

(11) 摘要长度决定抗冲突性。

(12) 报文摘要算法的复杂性决定单向性。

(13) 通过加密摘要产生用于实现完整性检测的消息鉴别码的前提是报文摘要算法具有抗冲突性。

(14) 不对称密钥算法不能够通过公钥推导出私钥。

(15) 公钥与某个用户之间的绑定无需证明。

(16) 不对称密钥算法的密钥长度和加密运算复杂性之间不成正比。

(17) 对称密钥算法和不对称密钥算法都需要足够长度的密钥。

(18) 分组密码的数据段长度和加密运算的复杂性有关。

(19) 数字信封是综合利用对称密钥加密算法和不对称密钥加密算法优势的一种方法。

(20) 网络安全中,源端鉴别、完整性检测和数字签名的重要性与数据加密相同。

4.2.2 自测题答案

1. 选择题答案

(1) D,由于解密算法公开,密文安全性完全依赖解密密钥的安全性。

(2) A,好的加密算法除了逐个尝试密钥空间中的所有密钥外,不应有其他破译密文的有效方法。

(3) A,解密算法遇到的挑战是能够以较小的代价用穷举法破译密文,网格计算符合这一条件。

(4) D,只能以穷举法破译密文说明加密算法可靠,密钥长度足够说明穷举法破译密文所需的时间很长,经得住网格计算考验说明目前还没有找到以较小的代价用穷举法破译密文的方法。

(5) D,不存在无法破译的密文,区别在于破译密文付出的代价和所需的时间。

(6) D,网络安全中,加密算法不再仅仅用于加密数据。

(7) D,这一点会使得报文摘要算法无法实现。

(8) D,分组密码是对称密钥加密算法,加密密钥和解密密钥相同。

(9) C,RSA 加密运算不用替代和置换,明文和密文长度之间的关系是变化的,一般不会相同。

(10) D,A、B 和 C 三项保证数字签名的唯一性和第三方的可证明性,这两项特性都是数字签名的先决条件。

(11) A,由于报文摘要算法的抗冲突性,使得报文摘要和报文之间的关联性得到保证。

(12) D,流密码是 4 项中唯一属于对称密钥加密算法的密钥体制。

(13) A,RSA 属于不对称密钥算法。

(14) D,该项使得用不对称密钥算法加密数据的成本增加。

(15) B,该项使得用对称密钥算法加密数据的成本较小。

(16) D,这一项是对称密钥算法共同的特点,不是流密码特有的。

2. 填空题答案

(1) 对称密钥算法,不对称密钥算法,对称密钥算法,不对称密钥算法。

(2) 将明文分成固定长度的数据段,通过多次替代和置换完成加密运算,生成和明文数据段等长密文,DES,AES。

(3) 数据段长度,密钥长度,加密运算复杂度,密钥长度,密钥长度。

(4) 固定长度摘要,单向性,抗冲突性,轻微改变报文将导致摘要发生较大变化,完整性检测,源端鉴别,数字签名。

(5) 加密密钥和解密密钥不同,不能由一个密钥推导出另一个密钥,加密密钥公开,

解密密钥保密，加密对称密钥算法使用的密钥，身份鉴别，数字签名。

(6) 密钥分发困难，多对多通信持有的密钥数量大，数据保密性差。

(7) 完整性检测，源端鉴别，加密报文摘要后产生的密文。

3. 名词解释答案

s 数字信封	t 密钥
a 对称密钥算法	b 不对称密钥算法
g AES	h 穷举
c 分组密码	d 流密码
i 报文摘要算法	j MD5
k SHA-1	l HMAC
q 数字签名	r 身份鉴别
m 加密	n 解密
e RSA	f DES
o 完整性检测	p 源端鉴别

4. 判断题答案

(1) 对，分组密码和流密码的明文和密文等长。

(2) 对，穷举法通过尝试密钥空间中的每一个密钥才能确定解密密文的解密密钥。

(3) 对，运算复杂度必须大到无法通过对有限的明文、密文对进行数学分析解析出解密密钥。

(4) 错，没有不可破译的密文，区别在于破译密文付出的代价和所花的时间。

(5) 对，安全加密算法的条件是：或者破译密文付出的代价超过密文信息的价值，或者破译密文所需的时间超出密文的有效期。

(6) 错，还包括源端鉴别、完整性检测、身份鉴别和数字签名等其他用途。

(7) 错，对称密钥算法其中一项缺陷是安全分发密钥困难，即使流密码的一次一密往往也是由固定密钥和以明文方式传输给接收端的初始向量产生的。

(8) 对，虽然加密算法的复杂度已经大到只能用穷举法来破译密文，但获得大量不同数据模式的明文对应的密文对破译解密密钥还是有所帮助的。

(9) 对，密钥保护不是一件简单的事情，保证某个密钥长时间不外泄是困难的。

(10) 错，由于报文空间远大于报文摘要空间，存在大量有着相同摘要的不同报文，只是从计算可行性讲，根据某个报文求出另一个和其报文摘要相同的不同报文是不可能的。

(11) 对，摘要长度确定摘要空间大小，摘要空间越大，相同摘要的不同报文数越少。

(12) 对，复杂性必须大到不能通过摘要反推出报文。

(13) 对，抗冲突性保证在黑客无法做到篡改报文同时又修改摘要的情况下，接收端能够检测出对报文进行的任何篡改。

(14) 对，这是不对称密钥算法的基本原则之一。

(15) 错，如果黑客用自己的公钥冒充某个用户的公钥，则加密发送给该用户的数据都将被黑客解密。

(16) 对，增加密钥长度将急剧增加运算复杂度，这是不对称密钥算法不适合加密数

据的原因。

(17) 对，即使加密算法保证只能通过穷举法破译密文，足够长度的密钥才能使得穷举法破译密文需要足够长的时间。

(18) 对，数据段长度越长，加密运算复杂度越高。

(19) 对，用接收端公钥加密对称密钥较好地解决了对称密钥分发困难的问题。

(20) 对，网络安全中，加密算法的重要性得到更广泛的体现。

4.2.3 简答题解析

1. 简述安全加密算法的特点。

回答：一是加密运算必须足够复杂，除了通过穷举法破译密文外，没有其他更有效的破译密文的方法；二是密钥长度必须足够长，以此保证，使用普通计算机破译密文时，用穷举法破译密文所需的时间超出密文的有效期，使用高性能计算机破译密文时，破译密文付出的代价超出密文信息价值；三是经过广泛试验，证明无法通过网格计算以较小成本用穷举法破译密文。

2. 简述信息安全的基础是加密算法的理由。

回答：一是加密算法是保证信息存储和传输过程中保密性的基础；二是加密算法和报文摘要算法是实现信息存储和传输过程中完整性检测的基础；三是加密算法是实现网络环境中身份鉴别、源端鉴别和数字签名的基础，而这些功能是许多网络应用的实现基础。

3. 简述 RSA 的数学原理。

回答：RSA 公开密钥加密算法的可靠性基于大数因子分解困难的事实，即根据数论，求出两个大素数比较简单，但将它们的乘积分解开则极其困难。RSA 实现过程如下。

(1) 选择两个不同的、长度相近的大素数 p 和 q，使得 $n=p\times q$。

(2) 计算欧拉函数 $\Phi(n)=(p-1)\times(q-1)$。

(3) 从 $2\sim\Phi(n)-1$ 中选择一个与 $\Phi(n)$ 互素的数作为 e。

(4) 求出满足等式 $ed \bmod \Phi(n)=1$ 的 d。

公开密钥（简称公钥）$\mathrm{PK}=(e,n)$，秘密密钥（简称私钥）$\mathrm{SK}=(d,n)$，对于 $0\sim n-1$ 的整数 P，加密过程为 $Y=P^e \bmod n$，解密过程为 $P=Y^d \bmod n=(P^e)^d \bmod n=P^{ed} \bmod n$。

破译密文的前提是根据 (e,n) 求出 d，求出 d 需要求出 $\Phi(n)$，求出 $\Phi(n)$ 需要求出 p 和 q，由于大数因子分解困难，当 n 长度大于 1024 时，根据现有计算能力无法通过 n 分解出 p 和 q。

第5章 鉴别协议和数字签名

CHAPTER

5.1 知识要点

5.1.1 Internet 接入控制

1. 接入控制过程

用户接入 Internet 的过程如图 5.1 所示。用户使用的终端(称为用户终端)通过接入网络连接接入控制设备,由接入控制设备完成用户终端与接入控制设备之间的传输通路和 Internet 的连接。接入控制设备实现用户终端与接入控制设备之间的传输通路和 Internet 的连接的前提是确定用户为授权用户,通过为用户终端分配一个全球 IP 地址,并在路由表中动态建立用于绑定分配给用户终端的全球 IP 地址和用户终端与接入控制设备之间传输通路的路由项完成用户终端与接入控制设备之间的传输通路和 Internet 的连接的过程,因而实现 IP 分组接入网络与 Internet 之间的转发。由此可以得出,用户接入 Internet 的过程分为:建立用户终端与接入控制设备之间的传输通路;接入控制设备完成对用户的身份鉴别;接入控制设备为用户终端动态分配全球 IP 地址;接入控制设备在路由表中动态建立用于绑定分配给用户终端的全球 IP 地址和用户终端与接入控制设备之间传输通路的路由项。

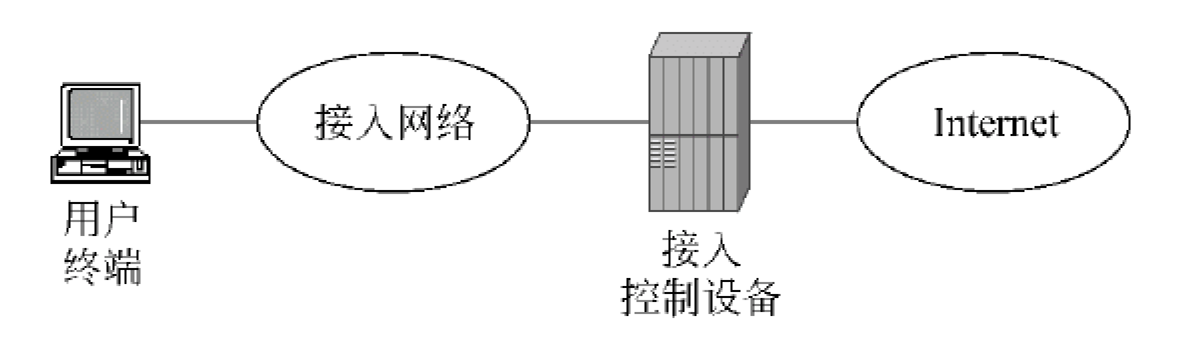


图 5.1 用户接入 Internet 方式

(1) 建立数据传输通路。

建立数据传输通路就是建立能够传输链路层帧的数据链路,不同类型的接入网络,建立数据链路的过程不同,如果 PSTN 作为接入网络,则建立数据链路的过程就是建立用户终端与接入控制设备之间的点对点语音信

道，并通过点对点协议（Point-to-Point Protocol，PPP）的链路控制协议（Link Control Protocol，LCP）建立传输 PPP 帧的 PPP 链路。如果是以太网，只要确定了两端的 MAC 地址，就可建立用于传输 MAC 帧的交换路径，但由于目前采用 PPPoE（PPP over Ethernet，基于以太网的 PPP）作为宽带接入控制协议，因此需要通过 PPPoE 建立类似用户终端与接入控制设备之间点对点语音信道的 PPP 会话，然后用 PPP 的 LCP 建立 PPP 链路。

（2）鉴别用户身份。

通过鉴别协议实现对用户身份的鉴别，但鉴别协议实现用户身份鉴别过程中需要交换的协议数据单元必须封装成数据链路对应的帧格式才能相互传输，因此，鉴别协议的协议数据单元只有作为 PPP 帧的净荷，才能在用户终端与接入控制设备之间相互传输。接入控制设备用于实现用户身份鉴别的鉴别协议主要有口令鉴别协议（Password Authentication Protocol，PAP）和挑战握手鉴别协议（Challenge Handshake Authentication Protocol，CHAP）。

（3）动态分配 IP 地址。

动态分配 IP 地址过程通过 IP 控制协议（IP Control Protocol，IPCP）实现。同样，IPCP 协议数据单元只有作为 PPP 帧的净荷，才能在用户终端与接入控制设备之间相互传输。

（4）建立动态路由项。

接入控制设备为了实现 IP 分组接入网络和 Internet 之间转发，必须建立用于绑定分配给用户终端的全球 IP 地址和用户终端与接入控制设备之间传输通路的路由项，传输通路可以是基于 PSTN 点对点语音信道的 PPP 链路，也可以是基于 PPP 会话的 PPP 链路。

2. PPP

PPP 顾名思义是基于点对点物理链路的链路层协议，它本来是针对拨号接入技术开发的接入控制协议，由两部分功能组成：一是基本链路层协议具有的功能，如定义 PPP 帧格式、检错和帧定界等；二是接入控制功能，如监测物理链路是否建立和经过信道传播的信号的质量是否符合数据传输要求，鉴别用户身份，动态分配 IP 地址。其实这些功能由三个独立的协议完成，它们分别是 LCP、PAP 或 CHAP 和 IPCP。在实现接入控制功能时，PPP 帧只是实现这三个协议对应的协议数据单元在用户终端和接入控制设备之间传输的载体。

（1）建立 PPP 链路。

LCP 建立 PPP 链路的主要目的：一是信道两端设备协商一些参数，如最大传送单元（Maximum Transfer Unit，MTU）值。二是监测信道是否存在，信号经过信道传播后的质量。三是确定信道两端设备实现用户身份鉴别时使用的鉴别协议。四是确定信道两端设备用于实现 IP 地址动态分配的协议。

（2）鉴别用户身份。

鉴别用户身份的过程就是判断用户是否拥有唯一标识其身份的用户标识信息，常见的用户标识信息是用户名和口令。鉴别协议需要保证用户标识信息的传输安全，PAP 这种用明文方式传输用户名和口令的鉴别协议一般不会用于需要保密用户标识信息的鉴别

过程。鉴别过程中需要交换的协议数据单元必须封装成 PPP 帧后，才能经过 PPP 链路传输，PPP 之所以称为接入控制协议，就是因为它除了是基于点对点信道的链路层协议外，还是鉴别协议和 IP 控制协议的承载协议。

（3）动态分配 IP 地址。

接入控制设备需要配置一个 IP 地址池，在建立用户终端与接入控制设备之间的数据传输通路，并由接入控制设备完成对用户的身份鉴别过程后，由用户终端通过 IPCP 向接入控制设备发出分配 IP 地址的请求，接入控制设备在 IP 地址池中选择一个未被分配的 IP 地址，并通过 IPCP 将该 IP 地址发送给用户终端，用户终端获取 IP 地址后才完成接入过程。接入控制设备在为用户终端分配 IP 地址后，需要在路由表中建立用于绑定该 IP 地址与用户终端和接入控制设备之间数据传输通路的路由项，这样，接入控制设备才能真正实现 IP 分组接入网络与 Internet 之间的转发。

3. PPPoE 的功能

PPP 作为承载协议，在建立用户终端与接入控制设备之间的 PPP 链路后，通过在用户终端和接入控制设备之间交换封装成 PPP 帧的鉴别协议对应的协议数据单元和 IPCP 对应的协议数据单元完成用户身份鉴别和用户终端 IP 地址分配过程，这是 PPP 成为 Internet 接入控制协议的原因。由于 PPP 是基于点对点信道的链路层协议，因此 PPP 只能成为以点对点信道连接用户终端和接入控制设备的接入网络的接入控制协议。当以太网成为接入网络时，由于用户终端与接入控制设备之间的传输通路是交换路径，因此并不能用 PPP 作为接入控制协议。PPPoE 的功能一是通过发现过程确定用户终端和接入控制设备的 MAC 地址，并用 PPP 会话标识符和两端 MAC 地址一起唯一标识某个 PPP 会话，二是实现用用户终端与接入控制设备之间的交换路径传输 PPP 帧的功能。

5.1.2 鉴别方式和类型

1. 本地鉴别和统一鉴别

（1）本地鉴别。

接入控制设备为了鉴别用户身份需要本地配置授权用户信息（用户名和口令），只有用户提供的鉴别信息与本地配置的某个授权用户的信息一致（相同用户名和口令），该用户才被允许接入 Internet。这种通过在接入控制设备创建本地用户库，用本地用户库中配置的授权用户信息作为鉴别接入用户依据的鉴别方式称为本地鉴别。

本地鉴别的好处是配置简单，不需要其他与接入控制有关的设备。坏处一是某个用户如果需要通过多种不同的接入控制设备接入 Internet，需要在这些接入控制设备中重复配置该用户的信息，如果某个用户需要通过图 5.2 中的以太网和 ADSL 接入 Internet，则需要在接入控制设备 1 和接入控制设备 2 中重复配置该用户的信息。二是接入用户信息需要分散到多个不同的接入控制设备，无法对接入用户集中管理。

（2）统一鉴别。

对于图 5.2 所示的 ISP 接入网络结构，本地鉴别方式的坏处是显而易见的，授权用户信息必须分散到多个不同的接入控制设备中，不利于对接入用户的集中管理。实际的接入控制过程一般采用统一鉴别方式，这种鉴别方式下，授权用户信息统一配置在鉴别服务

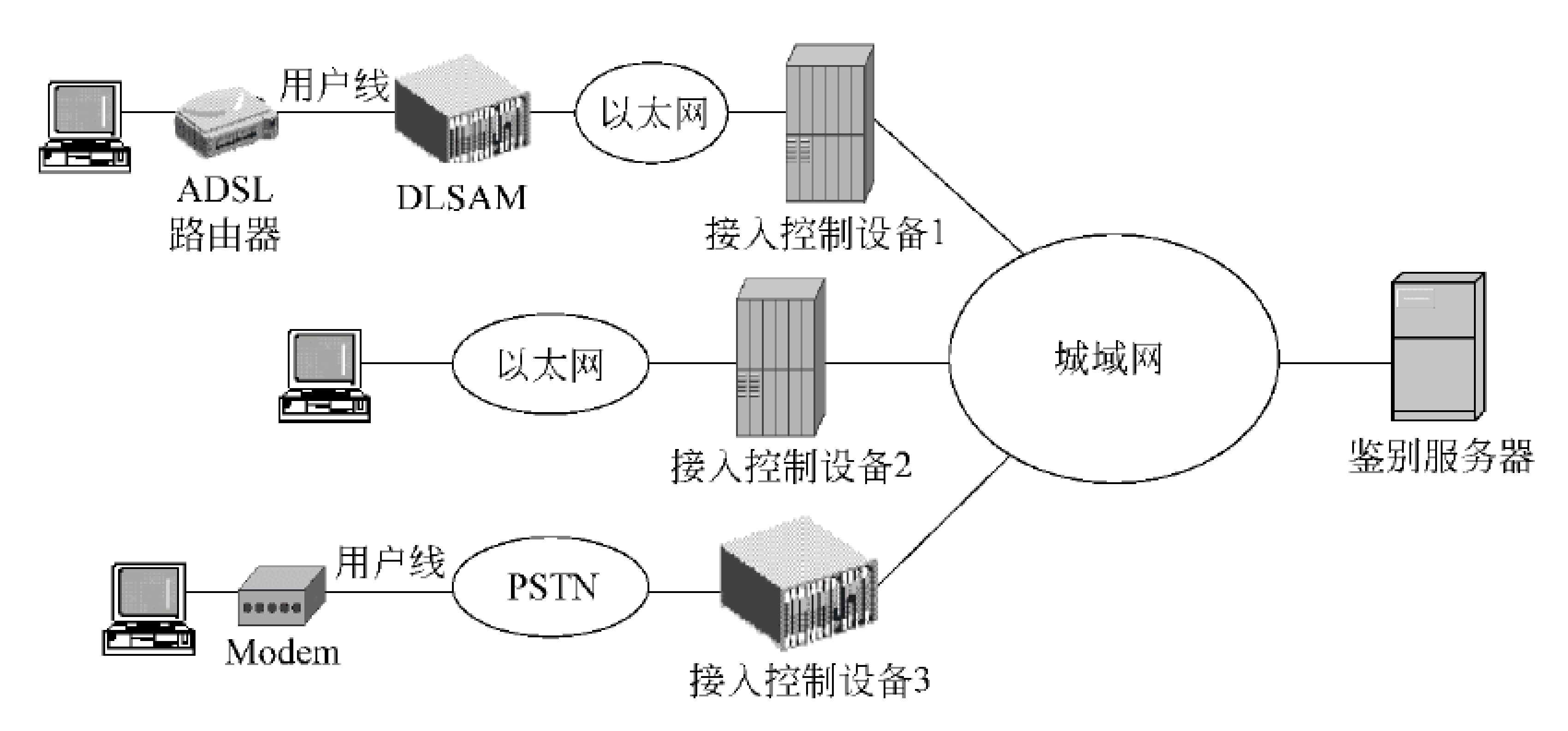


图 5.2　ISP 接入网络结构

器中，当用户向接入控制设备提供鉴别信息时，接入控制设备只是作为中继设备向鉴别服务器转发用户提供的鉴别信息。由鉴别服务器根据统一配置的授权用户信息完成对该用户的身份鉴别。

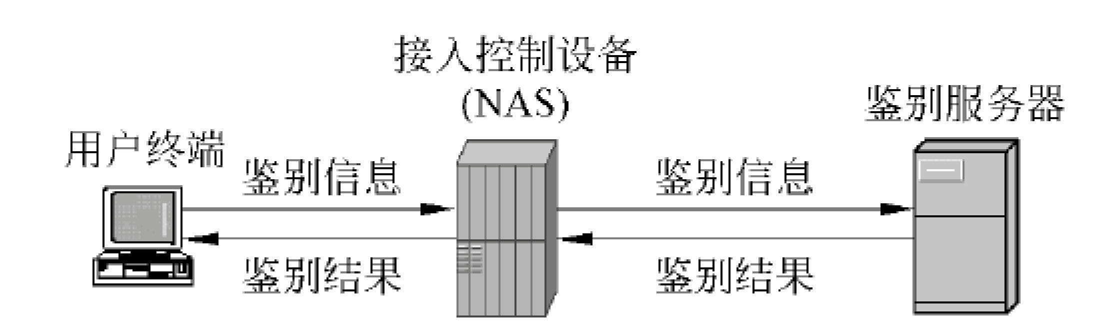


图 5.3　统一鉴别过程

统一鉴别过程如图 5.3 所示。由于接入控制设备与鉴别服务器之间是公共数据传输网络，接入控制设备与鉴别服务器之间相互交换的又是比较私密的用户鉴别信息，因此，一是需要对用户鉴别信息加密，二是需要相互鉴别对方身份。为实现这一功能，为每一对接入控制设备和鉴别服务器配置共享密钥，该共享密钥只有这一对接入控制设备和鉴别服务器知道，在接入控制设备中配置鉴别服务器的 IP 地址，并将该鉴别服务器标识信息与该共享密钥关联在一起。在鉴别服务器中配置接入控制设备的设备名和 IP 地址，并将这些设备标识信息与该共享密钥关联在一起。接入控制设备向鉴别服务器通过 RADIUS(Remote Authentication Dial In User Service，远程鉴别拨入用户服务)报文转发用户鉴别信息时，用明文方式给出设备名，用共享密钥和对称密钥加密算法加密用户鉴别信息。当鉴别服务器接收到该 RADIUS 报文，用该 RADIUS 报文的源 IP 地址和报文中明文方式给出的设备名检索设备标识信息，如果与某项设备标识信息匹配，用该项设备标识信息关联的共享密钥解密用户鉴别信息。一旦解密成功，接入控制设备的身份得到确认。由于只有与该共享密钥关联的鉴别服务器才能解密用户鉴别信息，因此，一旦解密用户鉴别信息成功，鉴别服务器的身份也得到确认。所以，在鉴别服务器回送给接入控制设备的鉴别结果中，一是同样需要用共享密钥加密一些信息，二是必须在鉴别结果中包含证明其已经成功解密用户鉴别信息的证据。

对于图 5.2 所示的 ISP 接入网络结构，需要单独为＜接入控制设备 1，鉴别服务器＞、＜接入控制设备 2，鉴别服务器＞和＜接入控制设备 3，鉴别服务器＞分配共享密钥，

在鉴别服务器中分别将这三个不同的共享密钥与这三个接入控制设备的设备名和 IP 地址关联在一起。

2. 接入鉴别、远程登录鉴别和交换机 802.1X 鉴别

网络中存在多种鉴别类型，如用户通过 PPP 接入 Internet 时进行的接入鉴别，管理用户通过 Telnet 远程登录网络设备时进行的远程登录鉴别，用户通过 802.1X 接入以太网交换机时进行的 802.1X 鉴别，所有这些鉴别类型既可以采用本地鉴别方式，也可以采用统一鉴别方式。将由鉴别服务器统一完成所有类型的身份鉴别的鉴别机制称为统一鉴别。

5.1.3　数字签名和身份鉴别

1. 数字签名实现原理

数字签名必须保证唯一性、关联性和可证明性，唯一性保证只有特定发送端能生成数字签名，关联性保证是对特定报文的数字签名，可证明性表明该数字签名的唯一性和与特定报文的关联性可以得到证明。

公开密钥算法中，公钥和私钥一一对应；私钥具有私密性，只有用户本身知道；如果公钥和用户之间的绑定关系能够被权威机构证明，具有不可否认性。因此，可用 D_{SK}(MD(P)) 作为用户 A 对特定报文 P 的数字签名，其中 D 是 RSA 解密算法，SK 是用户 A 私钥，MD 是报文摘要算法。依据如下：一是私钥 SK 只有用户 A 知道，因此只有用户 A 才能实现 D_{SKA}(MD(P))运算过程，保证了数字签名的唯一性；二是根据报文摘要算法的特性，即从计算可行性讲，其他用户无法生成某个报文 P'，$P \neq P'$，但 MD(P)＝MD(P')，因此 MD(P)只能是针对报文 P 的报文摘要算法的计算结果，保证了数字签名和报文 P 之间的关联性；三是数字签名能够被核实，因为公钥 PK 和私钥 SK 一一对应，如果公钥 PK 和用户 A 之间的绑定关系得到权威机构证明，一旦证明用公钥 PK 对数字签名进行加密运算后还原的结果(E_{PK}(数字签名))等于报文 P 的报文摘要(MD(P))，就可证明数字签名是 D_{SK}(MD(P))。

2. 源端鉴别

源端鉴别是接收端确定报文发送端是某个特定用户的过程。为了接收端能够实现源端鉴别，发送端在报文后面附上数字签名(D_{SK}(MD(P))，其中 D 是 RSA 解密算法，SK 是发送端私钥。接收端通过 RSA 加密算法 E 和公钥 PK 对数字签名进行加密运算还原出报文摘要(E_{PK}(数字签名)＝MD(P))，如果还原出的报文摘要与接收端对报文摘要运算后的结果相同，发送端身份得到确认，否则源端鉴别失败。图 5.4 所示源端鉴别过程能够成功的前提是接收端已经具有与某个特定用户关联的公钥，而且该特定用户与公钥之间的关联得到权威机构的证明。

3. 身份鉴别

身份鉴别是某个用户证明自己与某个标识符之间关联的过程，如某个用户证明自己的用户名为用户 A。采用对称密钥算法的身份鉴别机制大多在某个用户和鉴别者之间分配只有他们知道的共享密钥或口令，一旦某个用户能够向鉴别者提供该共享密钥或口令，用户身份得到确认。如果鉴别者需要完成多个用户的身份鉴别，必须保存一组＜用户名，

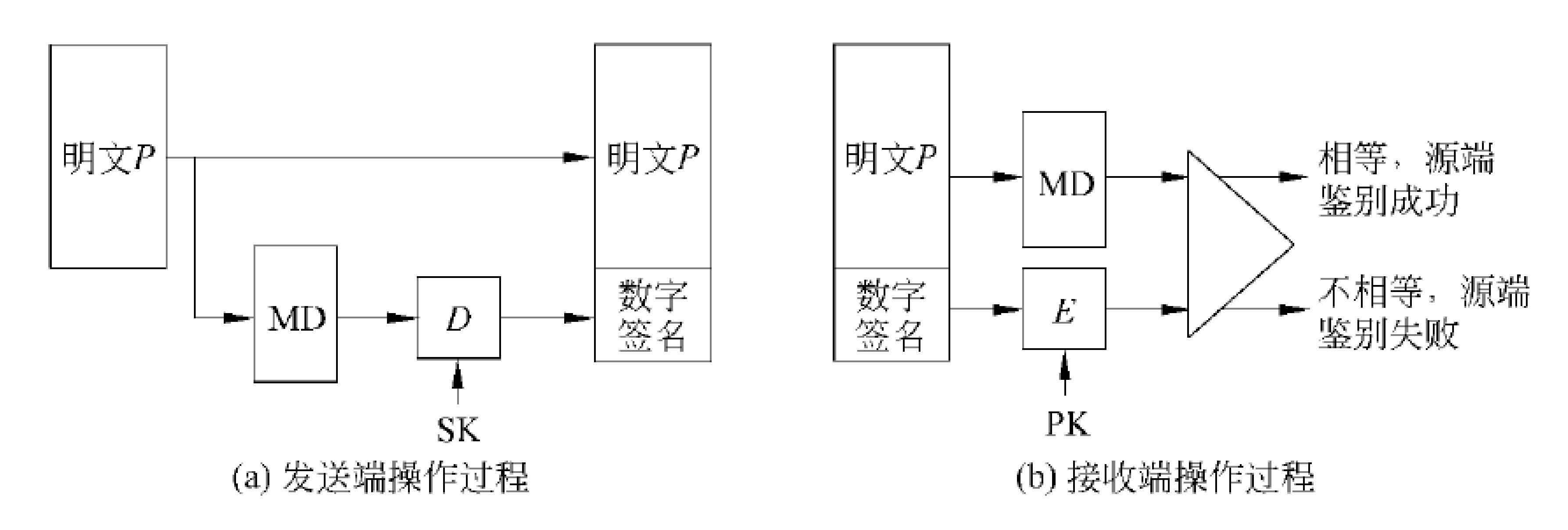


图 5.4 源端鉴别过程

共享密钥＞对，或者＜用户名，口令＞对。鉴别者保证这一组信息的保密性是身份鉴别有效进行的前提。

利用数字签名完成身份鉴别的过程如图 5.5 所示。用户 A 为了向鉴别者证明身份，首先向鉴别者发送证书链，证书链的作用是让鉴别者能够从它信任的认证中心颁发的证书开始，验证证明用户 A 和公钥 PK 关联的证书。对于图 5.6 所示的分层认证结构，假定鉴别者已经拥有证明认证中心 A(CA A)与公钥 PA 关联的证书，且已经证明证书的真实性，为了证明用户 A 与公钥 PK 之间的关联，用户 A 需要向鉴别者发送证书链 A＜＜C＞＞、C＜＜用户 A＞＞，鉴别者获得证书链后，用 CA A 关联的公钥 PA 证明用于证明 CA C 和公钥 PC 关联的证书的真实性，用 CA C 关联的公钥 PC 证明用于证明用户 A 与公钥 PK 关联的证书的真实性。



图 5.5 身份鉴别过程

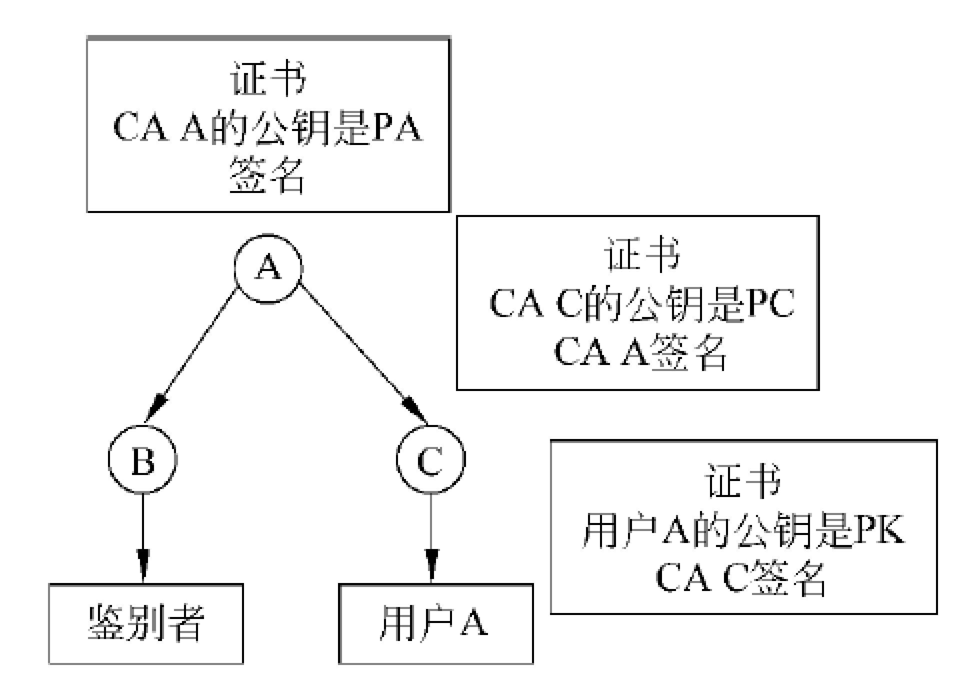


图 5.6 分层认证结构

一旦验证证明用户 A 和公钥 PK 关联的证书，鉴别者向用户 A 发送随机数 R，随机数 R 必须从一个很大的数字空间产生，保证规定时间内无法产生两个相同的随机数 R。用户 A 对随机数 R 数字签名，将随机数 R 的数字签名发送给鉴别者，如果鉴别者用 RSA 加密算法和用户 A 关联的公钥 PK 对数字签名加密运算后的结果与鉴别者对随机数 R

报文摘要运算后的结果相同，用户 A 的身份得到确认。

利用数字签名实现用户 A 身份鉴别的前提是用户 A 与公钥 PK 之间的关联得到权威机构证明；公钥 PK 与私钥 SK 一一对应；只有用户 A 拥有私钥 SK。这样，一旦某个用户证明拥有 PK 对应的私钥 SK，它的用户 A 的身份就得到确认。利用数字签名实现用户身份鉴别的最大好处是鉴别者无需存储任何有关用户的机密信息。

5.2　例题解析

5.2.1　自测题

1. 选择题

(1) 下面________与接入控制设备无关。

A. 建立用户终端与接入控制设备之间数据传输通路

B. 完成对接入用户的身份鉴别

C. 为用户终端分配 IP 地址

D. 由 ATM 网络实现两个物理上分割的以太网的中继功能

(2) 下面________与 PPP 作为接入控制协议无关。

A. 建立 PPP 链路时协商鉴别协议和网络控制协议

B. PPP 帧作为鉴别协议对应的协议数据单元的载体

C. PPP 帧作为 IP 控制协议对应的协议数据单元的载体

D. 实现 PPP 帧检错

(3) 对于 PPP，下面________描述是错误的。

A. 基于点对点信道的链路层协议

B. PSTN 作为接入网络时的接入控制协议

C. 通过 PPP over X 技术实现 PPP 帧经过多种类型的分组交换路径的传输过程

D. 通用的链路层协议

(4) 下述________不是 PPPoE 的功能。

A. 确定接入控制设备连接以太网端口的 MAC 地址

B. 分配 PPP 会话标识符

C. 将 PPP 帧封装成能够经过以太网实现用户终端和接入控制设备之间传输的 MAC 帧

D. 完成对用户终端的接入控制功能

(5) 以太网接入采用 PPPoE 的主要原因是________。

A. 接入控制设备需要通过 PPP 实现对用户终端的接入控制

B. 无法通过以太网建立用户终端与接入控制设备之间的数据传输通路

C. 以太网是短距离传输网络

D. 以太网是分组交换网络

(6) 用户终端通过以太网接入 Internet 不需要桥设备的原因是________。

A. 通过以太网建立用户终端与接入控制设备之间的交换路径

B. 用户终端通过 PPPoE 建立与接入控制设备之间的 PPP 会话

C. 接入控制设备需要通过 PPP 实现对用户终端的接入控制

D. 以太网是分组交换网络

(7) 用户终端通过 ADSL 接入 Internet 需要桥设备的原因是________。

A. 通过用户线连接两个物理上分割的以太网

B. 用户终端通过 PPPoE 建立与接入控制设备之间的 PPP 会话

C. 接入控制设备需要通过 PPP 实现对用户终端的接入控制

D. 以太网是分组交换网络

(8) 用户终端通过拨号接入方式接入 Internet 需要 Modem 的原因是________。

A. 用户线只能传输模拟信号

B. 通过呼叫连接建立过程建立用户终端与接入控制设备之间的点对点信道

C. 接入控制设备需要通过 PPP 实现对用户终端的接入控制

D. A 和 B

(9) 下述________和以太网接入无关。

A. 用以太网连接用户终端和接入控制设备

B. 用 PPPoE 实现 PPP 帧经过以太网在用户终端与接入控制设备之间传输

C. 接入控制设备用 PPP 完成对用户终端的接入控制

D. 用户终端与接入控制设备之间的交换路径由全双工点对点信道和交换机组成

(10) 图 5.7 是 NAT 的一个示例，根据图 5.7 中的信息，标号为①的箭头线所对应的方格内容应是________。

A. S=192.168.1.1:3105 D=202.113.64.2:8080

B. S=59.67.148.3:5234 D=202.113.64.2:8080

C. S=192.168.1.1:3105 D=59.67.148.3:5234

D. S=59.67.148.3:5234 D=192.168.1.1:3105

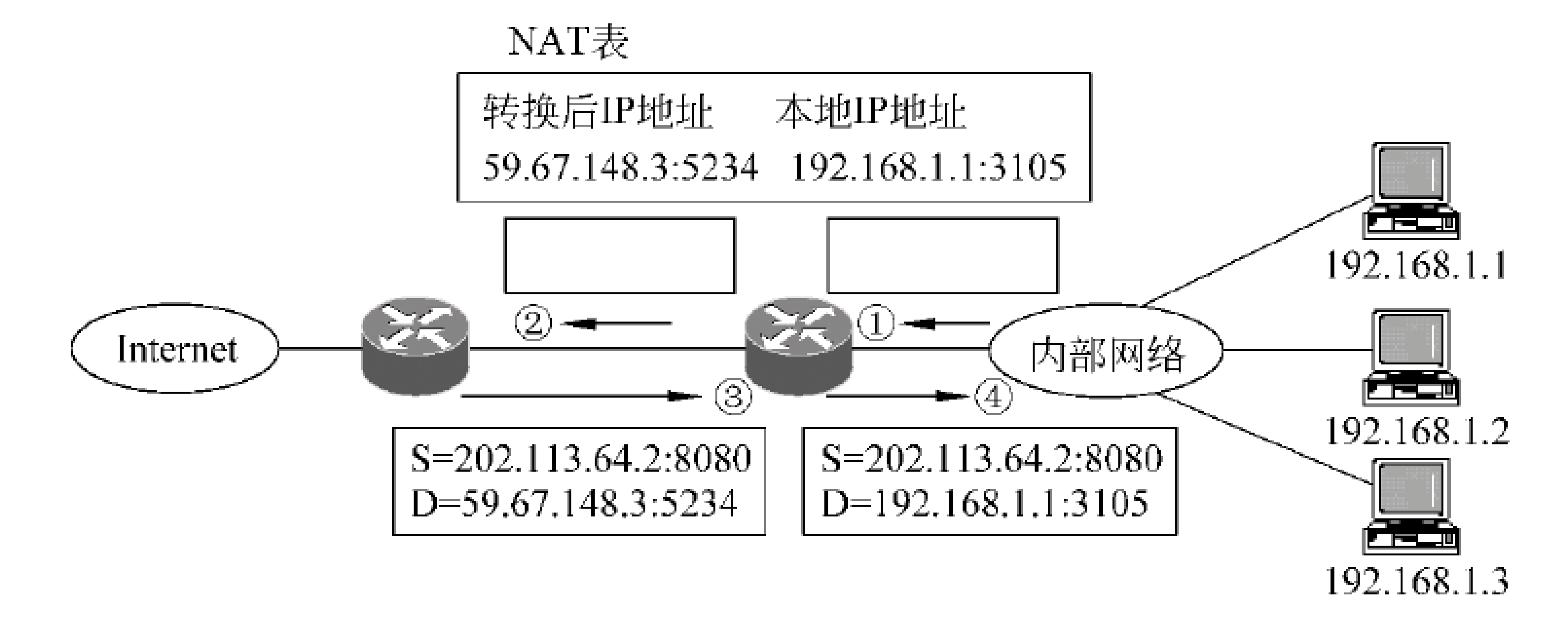


图 5.7 NAT 示例 1

(11) 图 5.8 是 NAT 的一个示例，根据图 5.8 中的信息，标号为④的箭头线所对应的方格内容应是________。

A. S=135.2.1.1:80

B. S=135.2.1.1:80

D=202.0.1.1:5001　　　　D=192.168.1.1:3342

C. S=135.2.1.1:5001　　　　D. S=192.168.1.1:3342

D=135.2.1.1:80　　　　D=135.2.1.1:80

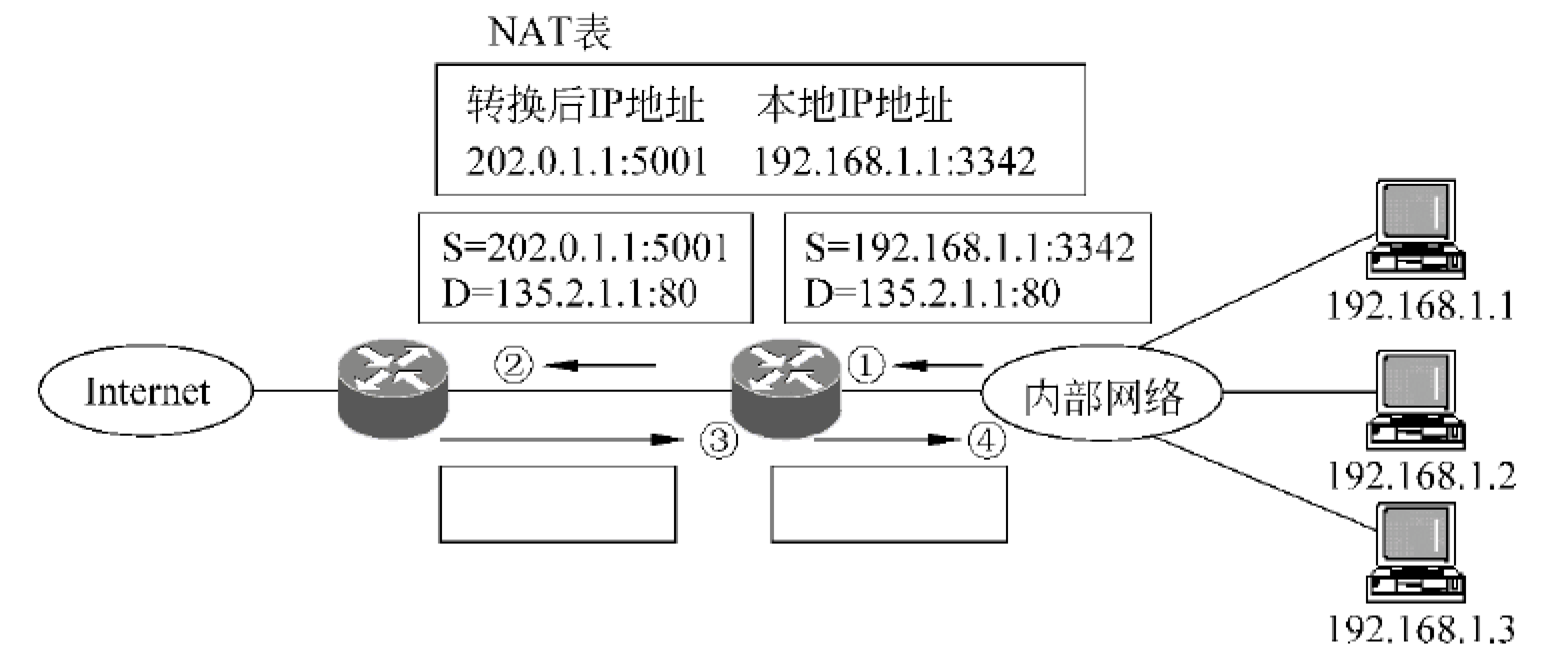


图 5.8　NAT 示例 2

（12）某家庭需要通过无线局域网将分布在不同房间的三台计算机接入 Internet，并且 ISP 只给其分配一个 IP 地址，这种情况下，应该选用的设备是 ________。

A. AP　　B. 无线路由器　　C. 无线网桥　　D. 交换机

（13）下述________是实现接入控制的前提。

A. 建立允许接入的授权用户的标识信息列表

B. 互连接入网络和 Internet 的路由器具有接入控制功能

C. 鉴别协议能够实现用户身份鉴别

D. 以上全是

（14）对于具有 802.1X 接入功能的设备，下述________描述是最贴切的。

A. 必须是路由器　　B. 必须是交换机

C. 可以是交换机　　D. 没有交换和路由功能的设备

（15）对于具有 PPP 接入功能的设备，下述________描述是最贴切的。

A. 必须是路由器　　B. 必须是交换机

C. 可以是交换机　　D. 没有交换和路由功能的设备

（16）下述________不是 RADIUS 具有的功能。

A. 实现对 NAS 源端鉴别

B. 加密用户鉴别信息

C. 经过 IP 网络实现鉴别协议对应的 PDU 的传输过程

D. 建立 NAS 与鉴别服务器之间的数据传输通路

（17）下述________不是鉴别服务器对应每一个 NAS 需要配置的信息。

A. 客户端名字　　B. 客户端 IP 地址

C. 共享密钥　　D. 对称密钥加密算法

（18）下述________不是对 Kerberos 票据的正确描述。

A. 票据用于证明客户对某个服务器的访问权限

B. 客户无法解密票据

C. 票据中授权客户访问的服务器能够解密票据
D. 票据用于证明发送票据的客户身份

(19) 下述________不是数字签名的特性。
A. 唯一性　　B. 与特定报文关联性
C. 可证明性　　D. 保密性

(20) 下述________不属于PKI的功能。
A. 用证书证明公钥与用户标识信息之间的关联
B. 管理证书
C. 生成公钥和私钥对
D. 分配共享密钥

(21) 关于鉴别协议,下述________描述是正确的。
A. 只能采用为每一对鉴别者和用户分配独立的共享密钥或口令
B. 只能采用证书和数字签名
C. 只能采用不属于A或B的鉴别方法
D. 允许采用A或B的鉴别方法

(22) IP Sec安全关联是________。
A. 单向的　　B. 双向的　　C. 无方向的　　D. 任意

(23) 下述________不属于IP Sec的功能。
A. 发送端鉴别　　B. 完整性检测　　C. 保密传输　　D. 差错控制

2. 填空题

(1) 用PPP实现用户终端接入Internet的控制过程分为________、________和________。

(2) 以太网接入的基本原理是________、________和________。

(3) 将局域网接入Internet需要________,对于局域网它是________,对于接入控制设备它等同于________。

(4) 接入控制设备除了是一个互连________和________的路由器,它还需具有对用户终端的________。

(5) 以太网接入采用PPPoE是因为________。ADSL接入方式下,接入网络由三部分组成,分别是________、________和________。ADSL路由器和DSLAM之间的用户线对用户终端和接入控制设备是________,因此ADSL接入同样采用PPPoE。

(6) 用户远程配置Cisco网络设备时,如果仅仅要求输入口令,这种鉴别方式称为________。如果要求输入在网络设备中配置的用户名和口令,这种鉴别方式称为________。如果要求输入在鉴别服务器中配置的用户名和口令,这种鉴别方式称为________。

(7) 鉴别服务器中,对于每一个NAS需要配置________、________和________,这些信息的作用有________和________。

(8) Kerberos中某个服务器允许某个客户对其进行访问的依据是________和________。

(9) 数字签名必须保证其________、________和 ________。

(10) 虽然鉴别协议多种多样,但是实现用户身份鉴别的机制无外乎 ________ 和 ________。

(11) 安全关联是________,建立安全关联的目的是________、________和 ________。

3. 名词解释

____ 802.1X	____ Kerberos
____接入网络	____接入控制过程
____安全关联	____ IP Sec
____ PPPoE	____接入控制设备
____ TLS	____ PKI
____ EAP	____ RADIUS
____证书	____认证中心
____以太网接入	____ PPP

(a) 用于实现用户终端与接入控制设备之间数据传输的网络。

(b) 用户终端接入 Internet 时,需要完成的建立用户终端与接入控制设备之间数据传输通路、对接入用户身份进行鉴别、为用户终端分配 IP 地址等控制过程。

(c) 这样一种用户终端接入 Internet 的方式,接入网络是以太网,用户终端与接入控制设备之间通过 PPPoE 建立的 PPP 会话实现 PPP 帧传输,接入控制设备通过 PPP 完成对用户终端的接入控制。

(d) 一种既是基于点对点信道的链路层协议,又具有用户终端接入控制功能的协议。

(e) 一种用于确定用户终端和接入控制设备以太网端口的 MAC 地址,实现 PPP 帧经过以太网在用户终端和接入控制设备之间传输的协议。

(f) 一种既是实现接入网络和 Internet 互连的路由器,又具有用户终端接入控制功能的设备。

(g) 一种能够为两端应用层实体提供双向身份鉴别、数据加密传输和完整性检测服务的传输层安全协议。

(h) 提供证书和公钥管理、证明用户标识符和公钥之间关联服务的公钥基础设施。

(i) 发送端 IP 实体与接收端 IP 实体之间建立的单向逻辑连接,其作用是保证单向传输的数据的保密性、完整性,实现源端鉴别和防止重放攻击。

(j) 为实现 IP 层数据安全传输而制定的一组安全协议。

(k) 一种通过扩展支持任何鉴别机制,同时又适用于多种不同传输网络的通用鉴别协议。

(l) 一种用于实现 NAS 和鉴别服务器之间用户鉴别信息和鉴别结果传输,并能够对 NAS 实现源端鉴别,保证经过 IP 网络传输的用户鉴别信息的保密性和完整性的应用层协议。

(m) 一种保证以太网端口只接收和转发授权用户发送的 MAC 帧的以太网端口接入控制协议。

(n) 一种对客户访问服务器资源过程实施控制的协议,主要功能是通过共享密钥对

客户身份进行鉴别，同时根据客户权限为客户分发用于访问服务器的票据。

(o) 一种由权威机构颁发，证明某个标识符与某个公钥之间绑定关系的文件。

(p) 一种颁发证明某个标识符与某个公钥之间绑定关系的证书的权威机构，同时提供证书管理、公钥和私钥对生成等服务。

4. 判断题

(1) 身份鉴别和源端鉴别是完全相同的。

(2) 数字签名可以实现源端鉴别。

(3) PPP Internet 接入控制过程将身份鉴别和源端鉴别有机集成在一起。

(4) 802.1X 以太网接入控制过程将身份鉴别和源端鉴别有机集成在一起。

(5) 以太网接入必须使用 PPPoE 协议。

(6) 通过共享密钥实现身份鉴别必须在鉴别者建立用户标识信息与共享密钥之间的关联。

(7) 通过证书和数字签名实现身份鉴别无需鉴别者存储任何有关用户的私密信息。

(8) IP Sec 安全关联是单向的。

(9) IP Sec 在 IP 层提供源端鉴别、数据加密传输和完整性检测等功能。

(10) 接入控制设备比普通路由器复杂。

5.2.2 自测题答案

1. 选择题答案

(1) D，接入控制设备将接入网络作为以太网，完成 A、B 和 C 的功能。

(2) D，D 的功能是 PPP 作为普通链路层协议具有的功能，不属于接入控制功能。

(3) D，PPP 既是基于点对点信道的链路层协议，同时又是接入控制协议，但不是通用链路层协议，实际上不存在通用的链路层协议。

(4) D，PPPoE 的功能主要用于实现 PPP 帧经过以太网在用户终端和接入控制设备之间传输，接入控制功能由 PPP 实现。

(5) A，因为采用 PPP，所以要解决 PPP 帧经过以太网在用户终端和接入控制设备之间传输的问题。

(6) A，用户终端和接入控制设备之间直接通过以太网实现 MAC 帧传输。

(7) A，ADSL 路由器和 DSLAM 是互连以太网和基于用户线的 ATM PVC 的桥设备，ADSL 接入网络是由基于用户线的 ATM PVC 连接的两个物理上分割的以太网组成的。

(8) D，一是需要 Modem 通过呼叫连接建立过程建立用户终端与接入控制设备之间的语音信道，二是需要 Modem 实现用户终端串行口输出的数字信号与用户线传输的模拟信号之间的相互转换。

(9) D，以太网作为接入网络时，基本功能是实现用户终端与接入控制设备之间的 MAC 帧传输，但没有要求用户终端与接入控制设备之间的交换路径必须由全双工点对点信道和交换机组成。

(10) A，根据图 5.7 中标号为③和④箭头线所对应的方格内容可以确定该次会话的

发起端为192.168.1.1:3105,响应端为202.113.64.2:8080,因此标号为①的箭头线所对应的方格内容应该是源IP地址和源端口号为192.168.1.1:3105,目的IP地址和目的端口号为202.113.64.2:8080。

(11) B,根据图5.8中标号为①箭头线所对应的方格内容可以确定该次会话的发起端为192.168.1.1:3342,响应端为135.2.1.1:80,因此标号为④的箭头线所对应的方格内容应该是源IP地址和源端口号为135.2.1.1:80,目的IP地址和目的端口号为192.168.1.1:3342。

(12) B,无线路由器是一种既能无线连接内部局域网中的移动终端,又能实现将内部局域网接入Internet的边缘路由器。

(13) D,A和C是实现身份鉴别必须的,B是接入网络结构所要求的。

(14) C,802.1X是以太网端口接入控制协议,具有以太网端口的设备都可具有802.1X接入控制功能。

(15) A,具有PPP接入控制功能的设备必须是互连接入网络和Internet的路由器。

(16) D,这一项不是应用层协议的功能。

(17) D,RADIUS加密数据只使用共享密钥和报文摘要算法。

(18) D,票据不具有源端鉴别功能。客户端通过发送鉴别信息证实自己的身份。

(19) D,数字签名自身无需保密。

(20) D,PKI是证书和公钥管理平台。

(21) D,一种鉴别协议同时支持多种鉴别方法。

(22) A,IP Sec安全关联是单向的,发送端至接收端。

(23) D,IP Sec不提供差错控制功能。

2. 填空题答案

(1) 建立PPP链路,完成接入用户身份鉴别,分配IP地址。

(2) 以太网实现用户终端与接入控制设备之间的MAC帧传输,PPPoE实现PPP帧封装成MAC帧后在用户终端与接入控制设备之间传输,PPP实现对用户终端的接入控制。

(3) 路由器,边缘路由器,用户终端。

(4) 接入网络,Internet,接入控制功能。

(5) 需要实现PPP帧经过以太网在用户终端和接入控制设备之间传输,互连用户终端和ADSL路由器的以太网,互连ADSL路由器和DSLAM的基于用户线的ATM PVC,互连DSLAM和接入控制设备的以太网,透明的。

(6) 口令鉴别,本地鉴别,统一鉴别。

(7) 客户端名字,客户端IP地址,共享密钥,客户端源端鉴别,用户鉴别信息加密传输。

(8) 拥有授权访问该服务器的票据,证实客户是票据拥有者的鉴别信息。

(9) 唯一性,与特定报文关联性,可证明性。

(10) 为每一对鉴别者和用户分配独立的共享密钥或口令,采用证书和数字签名。

(11) 单向的,发送端鉴别,加密传输,完整性检测。

3. 名词解释答案

m 802.1X	n Kerberos
a 接入网络	b 接入控制过程
i 安全关联	j IP Sec
e PPPoE	f 接入控制设备
g TLS	h PKI
k EAP	l RADIUS
o 证书	p 认证中心
c 以太网接入	d PPP

4. 对错题答案

(1) 错,源端鉴别是确认报文发送端,身份鉴别是确认某个用户与某个标识符之间关联,或许有时采用相同的鉴别方法,但过程和目的不同。

(2) 对,能够用数字签名确认报文发送端。

(3) 对,身份鉴别过程将 IP 地址和连接用户终端的点对点信道或 PPP 会话与某个用户绑定在一起,可以通过 IP 分组的源 IP 地址和传输该 IP 分组的点对点信道或 PPP 会话确定 IP 分组的发送端。

(4) 对,身份鉴别过程将 MAC 地址与某个用户绑定在一起,可以通过 MAC 帧的源 MAC 地址确定 MAC 帧的发送端。

(5) 错,接入控制设备用 PPP 实现对用户终端的接入控制时才需要 PPPoE,接入控制设备可以采用其他接入控制协议实现对用户终端的接入控制。

(6) 对,某个用户知道共享密钥是证明与该共享密钥关联的标识符就是该用户标识符的唯一依据。

(7) 对,PKI 能够证明标识符与公钥之间的关联,用户只要通过数字签名提供拥有公钥对应的私钥的证据,即可证明与该公钥关联的标识符就是该用户标识符。

(8) 对,IP Sec 安全关联是单向的,发送端至接收端方向。

(9) 对,IP Sec 的目的就是在 IP 层提供安全传输功能。

(10) 对,接入控制设备除了具有普通路由器的功能外,还需具有接入控制功能。

5.2.3 简答题解析

1. 简述接入控制设备的作用。

回答:接入控制设备的作用:一是作为普通路由器实现接入网络与 Internet 的互连;二是实现对用户终端的接入控制,主要功能包括鉴别接入用户身份、动态分配 IP 地址、建立用于指明通往用户终端的传输路径的路由项。

2. 简述 PPPoE 的基本功能。

回答:PPPoE 的基本功能是实现 PPP 帧经过以太网在用户终端与接入控制设备之间传输,主要功能包括通过发现过程确定用户终端和接入控制设备的 MAC 地址,创建 PPP 会话并分配 PPP 会话标识符,将 PPP 帧封装成 MAC 帧。

3. 简述鉴别协议实现用户身份鉴别的过程。

回答：用户首先到ISP注册，同时约定用于标识用户身份的标识信息，接入控制设备通过配置获得，或可以访问到用户标识信息，用户通过鉴别协议向接入控制设备提供标识信息，如果用户提供的标识信息与接入控制设备中和某个注册用户绑定的标识信息相同，用户被确定为授权用户。

4. 简述802.1X实现以太网交换机接入控制的过程。

回答：①鉴别者或者鉴别服务器配置授权用户标识信息。②用户提供标识信息，如果用户提供的标识信息与某个授权用户的标识信息相同，用户身份得到确认。③将身份鉴别过程中用户向鉴别者传输鉴别信息的MAC帧的源MAC地址作为源端鉴别的依据，所有源MAC地址为该MAC地址的MAC帧确定为该授权用户发送的MAC帧。

5. 简述PPP实现Internet接入控制的过程。

回答：①鉴别者或者鉴别服务器配置授权用户标识信息。②用户提供标识信息，如果用户提供的标识信息与某个授权用户的标识信息相同，用户身份得到确认。③将为用户分配的IP地址和建立的用户终端与接入控制设备之间的点对点信道或PPP会话作为源端鉴别的依据，所有源IP地址为该IP地址且经过该点对点信道或PPP会话到达接入控制设备的IP分组确定为该授权用户发送的IP分组。

6. 简述资源访问控制原理及过程。

回答：①配置授权用户标识信息。②为每一个授权用户分配资源访问权限。③一旦用户提出资源访问请求，首先鉴别该用户身份，鉴别用户身份的过程就是确定该用户提供的标识信息是否和配置的某个授权用户的标识信息相同的过程。④确定用户提出的资源访问请求是否符合分配该用户的资源访问权限。⑤在确定该用户为授权用户且具有资源访问请求中要求的资源访问权限后，完成资源访问过程。

5.2.4 综合题解析

网络结构如图5.9所示，R1、R3和R5为接入控制设备，RADIUS服务器为鉴别服务器，要求：

① 实现由鉴别服务器统一鉴别用户身份。

② R1、R3和R5作为NAS，完成统一鉴别所需的相关配置，同时在鉴别服务器中配置有关NAS的信息。

③ 由鉴别服务器完成各个路由器远程登录用户的身份鉴别，完成路由器有关远程登录统一鉴别的配置，同时在鉴别服务器中配置路由器相关信息。

④ 简述Internet接入控制过程。

⑤ 简述路由器远程登录过程。

解析：① 采用统一鉴别方式，在鉴别服务器中统一配置授权用户信息：用户名和口令，如＜aaa1，bbb1＞，其中aaa1是用户名，bbb1是口令。

② 接入控制设备鉴别用户身份的鉴别方式分为本地鉴别和统一鉴别，必须将PPP Internet接入控制过程中采用的鉴别方式定义为统一鉴别。同时，需要配置RADIUS服务器IP地址和只用于该接入控制设备与该RADIUS服务器的共享密钥。在RADIUS

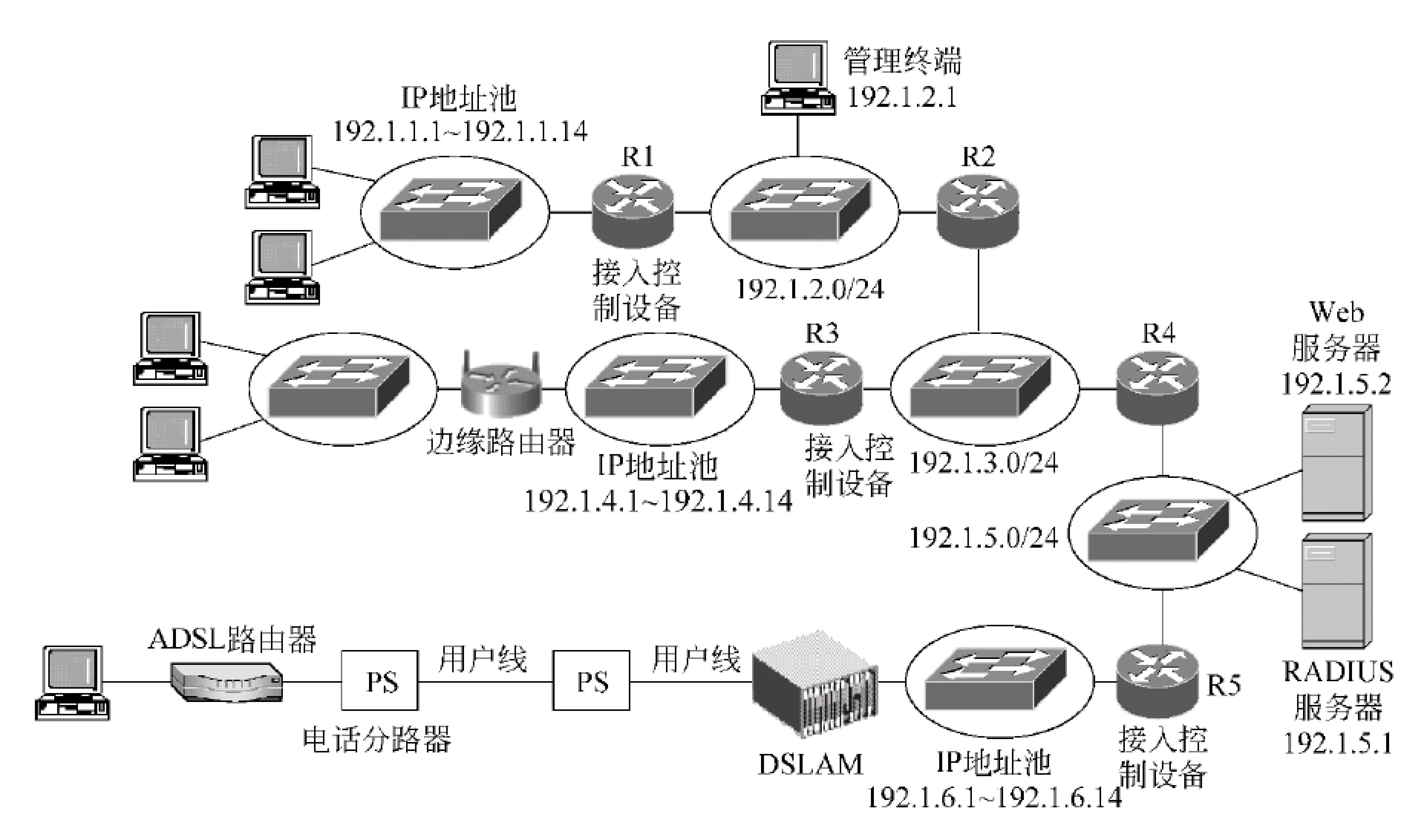


图 5.9　综合统一鉴别过程

服务器中为每一个接入控制设备(在 RADIUS 中称为 NAS)配置客户端名字、IP 地址和共享密钥,该共享密钥必须与该接入控制设备中配置的共享密钥相同。

③ 路由器鉴别远程登录用户身份的鉴别方式分为口令鉴别、本地鉴别和统一鉴别。口令鉴别方式为所有远程登录用户分配同一个登录口令。本地鉴别方式需要在路由器中创建本地用户库,配置授权用户信息:用户名和口令,只有当提供的用户信息与本地配置的某个授权用户信息相同时,才能成功远程登录该路由器。统一鉴别使用鉴别服务器中配置的授权用户信息,路由器必须将远程登录鉴别方式定义为统一鉴别,如果路由器还没有配置有关 RADIUS 服务器信息,需要配置 RADIUS 服务器 IP 地址和只用于该路由器与该 RADIUS 服务器的共享密钥。在 RADIUS 服务器中为该路由器配置客户端名字、IP 地址和共享密钥,该共享密钥必须与该路由器中配置的共享密钥相同。

④ 用户终端启动 PPPoE 连接程序,输入用户名和口令,首先通过 PPPoE 建立用户终端与接入控制设备之间的 PPP 会话,然后通过 PPP 在 PPP 会话基础上建立 PPP 链路。用户终端和接入控制设备之间建立 PPP 链路后,如果接入控制设备配置的接入用户鉴别机制为 CHAP,向用户终端发送随机数 C,用户计算出 MD5(C‖口令)后,连同明文方式的用户名一起发送给接入控制设备。由于接入控制设备配置的鉴别方式为统一鉴别方式,接入控制设备将这些信息连同随机数 C 和接入控制设备名一起封装成 RADIUS 报文,并将 RADIUS 报文发送给 RADIUS 服务器。

RADIUS 服务器首先根据接入控制设备名和 RADIUS 报文的源 IP 地址确定 NAS,然后通过共享密钥解密出用户终端发送的鉴别信息,根据用户名确定口令,根据口令重新计算 MD5(C‖口令),如果计算结果与用户发送的鉴别信息相同,向接入控制设备发送允许接入报文,接入控制设备向用户终端发送鉴别成功报文。整个统一鉴别过程如图 5.10 所示。

完成鉴别过程后,进行 IP 地址分配和路由项建立过程。

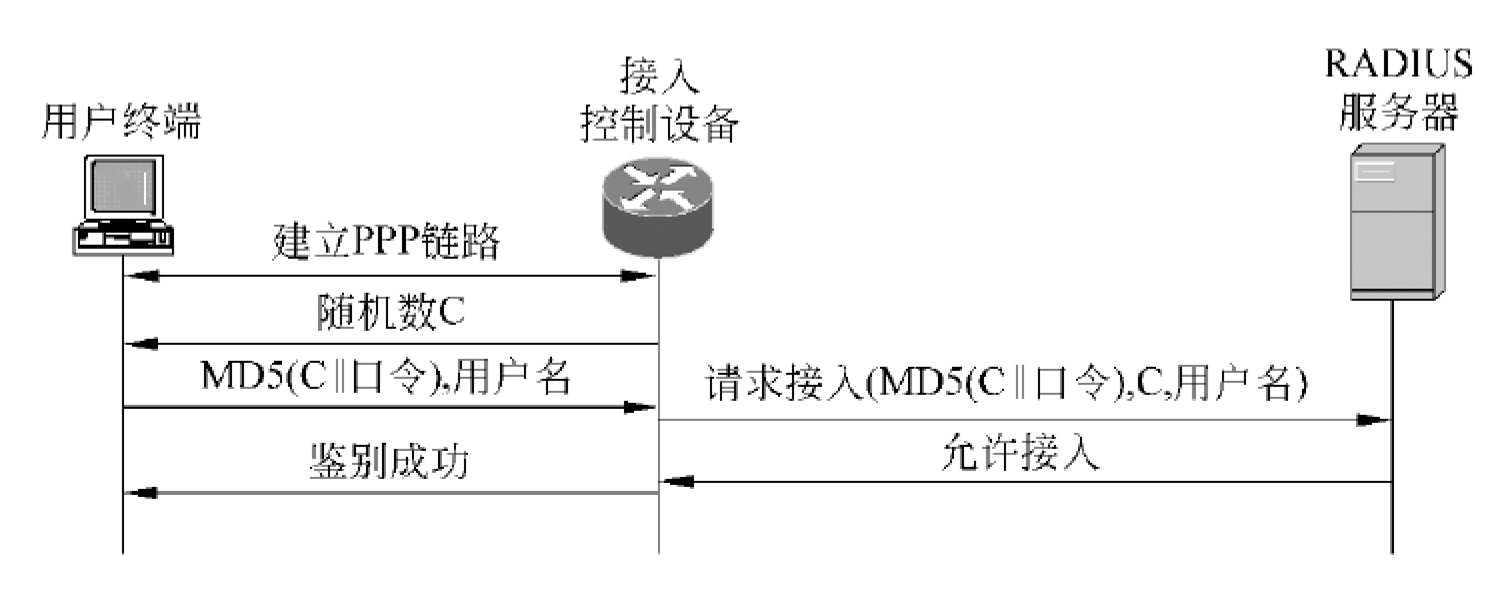


图 5.10　CHAP 鉴别过程

⑤ 用户启动 Telnet 客户端，Telnet 客户端建立与路由器之间的 TCP 连接，然后要求用户输入用户名和口令，将用户输入的用户名和口令传输给路由器，由路由器将其封装成 RADIUS 报文，并将 RADIUS 报文发送给 RADIUS 服务器。

RADIUS 服务器首先根据路由器名和 RADIUS 报文的源 IP 地址确定路由器，然后通过共享密钥解密出用户名和口令，如果在 RADIUS 服务器配置的授权用户信息中找到与该用户名和口令对相同的授权用户信息，向路由器发送允许接入报文，路由器向用户发送远程登录成功信息。

5.3　实　　验

5.3.1　终端接入本地鉴别实验

1. 实验内容

(1) 完成本地鉴别配置。

(2) 完成终端接入配置。

(3) 验证终端接入过程。

2. 网络结构

网络结构如图 5.11 所示。终端 A 和 B 采用以太网接入 Internet 方式，路由器 R1 为接入控制设备，通过 PPP 完成对接入终端的身份鉴别和 IP 地址分配，并在路由表中动态生成将分配给接入终端的 IP 地址与互连接入终端和路由器 R1 的 PPP 会话绑定在一起的路由项，PPP 会话通过 PPPoE 创建。

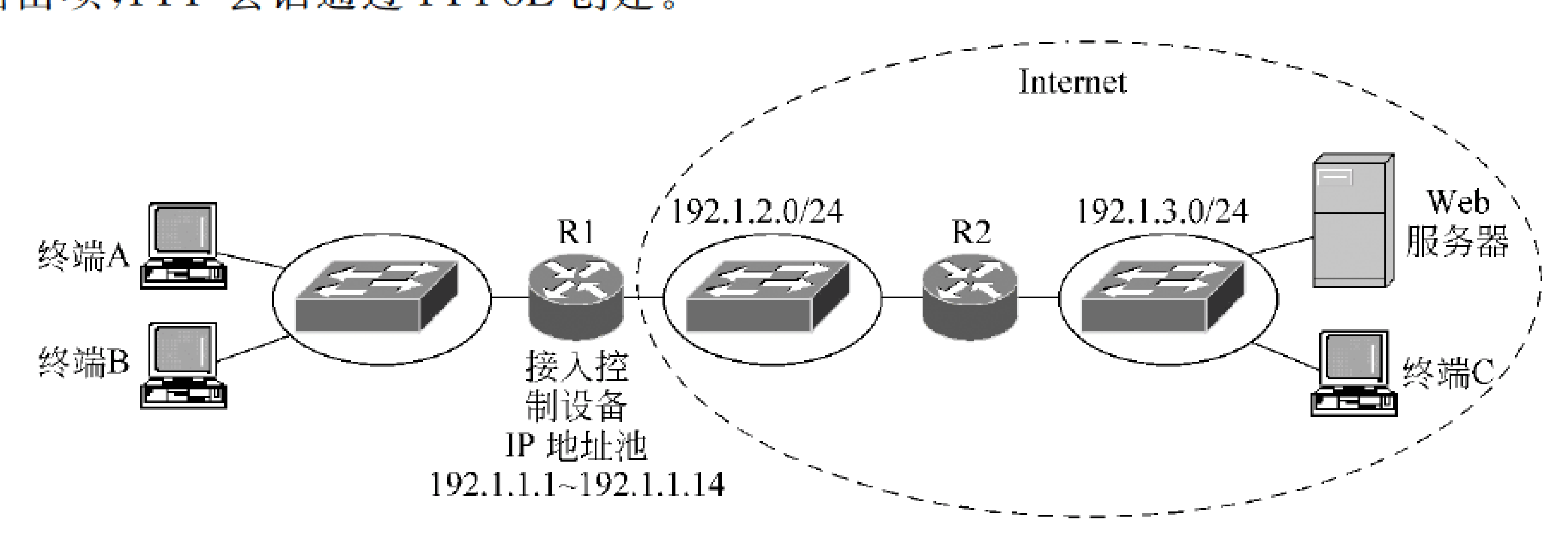


图 5.11　终端接入 Internet 过程

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 5.11 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 5.12 所示。

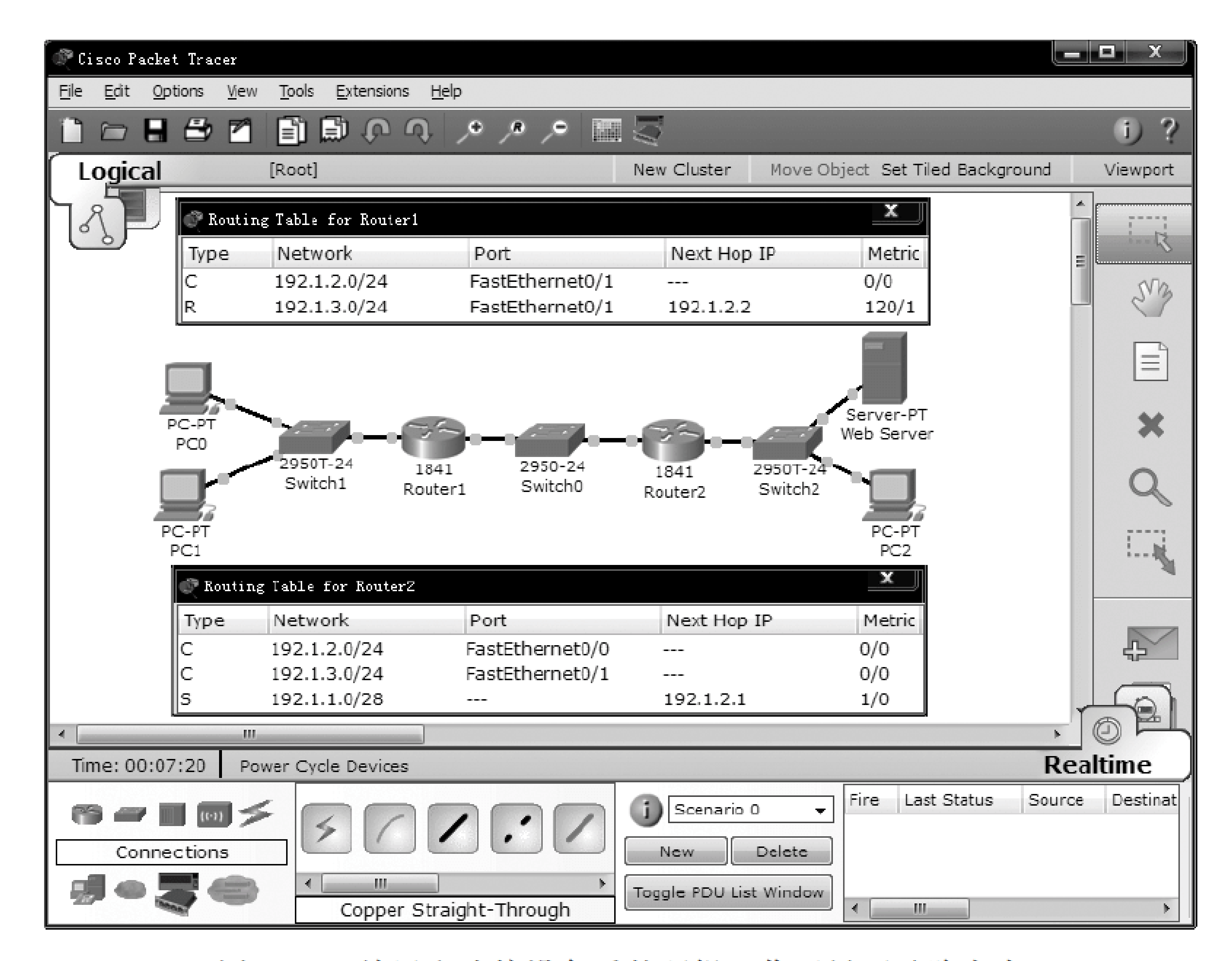


图 5.12 放置和连接设备后的逻辑工作区界面及路由表

(2) 完成路由器接口 IP 地址和子网掩码配置，完成各个路由器路由协议配置和静态路由项配置，生成图 5.12 所示的路由表。需要指出的是，Router1 指向 PC0 和 PC1 的路由项在完成接入控制过程后动态建立，但 Router2 需配置用于指明通往网络 192.1.1.0/28 传输路径的静态路由项。

(3) 通过在全局配置模式命令提示符下输入命令"username 用户名 password 口令"创建两个注册用户。用命令"aaa new-model"启动身份鉴别机制，用命令"aaa authentication ppp a1 local"定义名为 a1 的鉴别列表，该鉴别列表确定 PPP 鉴别用户身份时使用本地鉴别机制。本地鉴别机制用本地注册用户库信息鉴别用户身份。

(4) 将以 PSTN 为接入网络的接入 Internet 方式称为拨号接入方式，以太网、ADSL 和 VPN 接入过程其实都仿真拨号接入过程，因此，Cisco 将通过用 PPP 会话或第 2 层隧道仿真 PSTN 点对点信道，以此为基础用 PPP 实现接入控制的接入方式统称为虚拟拨号接入方式，作为接入网络的以太网、ADSL 和 IP 网络称为虚拟专用拨号网络(Virtual Private Dialup Networks，VPDN)。只要是采用虚拟拨号接入方式，需要用命令"vpdn enable"启动虚拟专用拨号网络功能，并定义与这次使用的虚拟拨号接入方式相对应的虚拟专用拨号网络的相关属性。

(5) 用命令"ip local pool c1 192.1.1.1 192.1.1.14"定义 IP 地址池 192.1.1.1～192.1.1.14，其中 c1 为该 IP 地址池的名字，以后可以通过名字 c1 引用该 IP 地址池。

(6) 用户终端一旦完成接入过程，接入控制设备路由器 Router1 与用户终端之间相当于建立了虚拟点对点线路，路由器 Router1 等同于创建了用于连接虚拟点对点线路的虚拟接口，因此，通过定义虚拟接口模板的方式定义完成虚拟点对点线路建立所需要的相关参数。

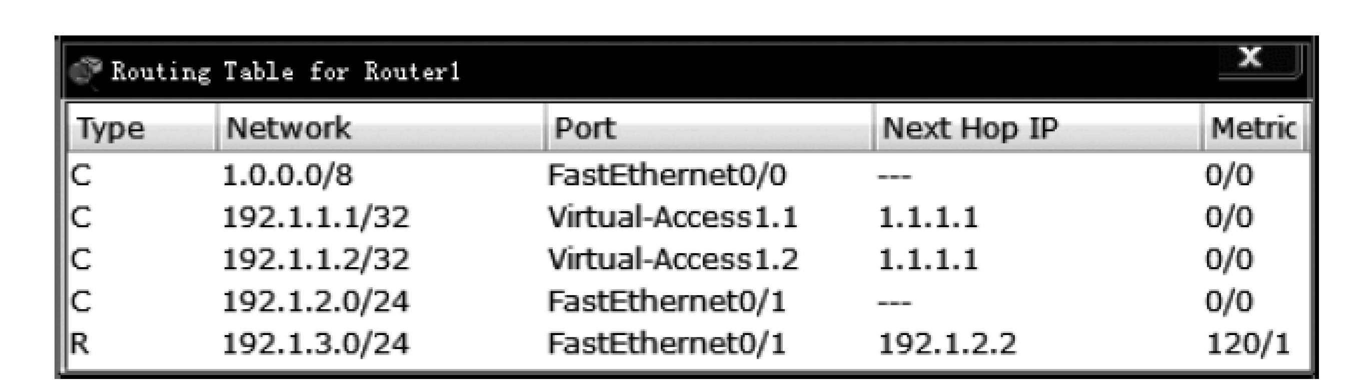
(7) 通过命令“pppoe enable”，在路由器连接作为接入网络的以太网接口 FastEthernet0/0 启动基于 PPP 会话用 PPP 实现接入控制的虚拟拨号接入方式。

(8) 完成路由器 Router1 有关配置后，用户终端启动 PPPoE 连接程序，输入用户名和口令，完成用户终端 PPPoE 接入过程。PPPoE 连接程序界面如图 5.13 所示。



图 5.13　PC0 PPPoE 连接程序界面

(9) 查看路由器 Router1 的路由表，路由器 Router1 直接通过虚拟接口连接了用户终端，并将连接用户终端的虚拟接口和分配给用户终端的 IP 地址绑定在一起，分配给用户终端的 IP 地址从 IP 地址池中选择。路由器 Router1 的路由表如图 5.14 所示，命令“ip unnumbered FastEthernet0/0”指定，如果虚拟接口产生并发送报文，可以将 Router1 接口 FastEthernet0/0 的 IP 地址作为该报文的源 IP 地址，这样指定似乎将 Router1 接口 FastEthernet0/0 作为虚拟接口向终端传输 IP 分组的下一跳。


Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	1.0.0.0/8	FastEthernet0/0	---	0/0
C	192.1.1.1/32	Virtual-Access1.1	1.1.1.1	0/0
C	192.1.1.2/32	Virtual-Access1.2	1.1.1.1	0/0
C	192.1.2.0/24	FastEthernet0/1	---	0/0
R	192.1.3.0/24	FastEthernet0/1	192.1.2.2	120/1

图 5.14　PC0 和 PC1 接入后的 Router1 路由表

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 1.1.1.1 255.0.0.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.1 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#exit
Router(config)#aaa new-model              (启动鉴别机制)
Router(config)#aaa authentication ppp a1 local
                    (定义名为 a1 的鉴别列表,鉴别列表指定 PPP 鉴别用户身份时使用本地鉴别机制)
Router(config)#username aaa1 password bbb1
                                          (在本地注册用户库创建一个用户<aaa1,bbb1>)
Router(config)#username aaa2 password bbb2
Router(config)#vpdn enable                (启动虚拟专用拨号网络功能)
Router(config)#vpdn-group b1
                                    (定义采用 PPP 会话实现接入的虚拟专用拨号网络的相关属性)
Router(config-vpdn)#accept-dialin        (定义允许接入的虚拟拨号接入方式)
Router(config-vpdn-acc-in)#protocol pppoe
                                          (允许采用 PPP 会话的虚拟拨号接入方式)
Router(config-vpdn-acc-in)#virtual-template 1
                                          (定义与该虚拟拨号接入方式关联的虚拟接口模板)
Router(config-vpdn-acc-in)#exit          (退出虚拟拨号接入方式相关属性的配置过程)
Router(config-vpdn)#exit                  (退出虚拟专用拨号网络相关属性的配置过程)
Router(config)#ip local pool c1 192.1.1.1 192.1.1.14
                                    (定义 IP 地址池 192.1.1.1～192.1.1.14,c1 是该 IP 地址池名)
Router(config)#interface virtual-template 1
                                         (配置与该虚拟拨号接入方式关联的虚拟接口模板。所有
                                          连接虚拟点对点线路的虚拟接口通过下述配置项创建)
Router(config-if)#ip unnumbered FastEthernet0/0
                                        (连接虚拟点对点线路的虚拟接口不配置 IP 地址和子网掩
                                         码,如果需要,使用接口 FastEthernet0/0 的 IP 地址)
Router(config-if)#peer default ip address pool c1
                                       (从名为 c1 的 IP 地址池中选择分配给用户终端的 IP 地址)
Router(config-if)#ppp authentication chap a1
                   (采用鉴别协议 CHAP 鉴别接入用户身份,使用名为 a1 的鉴别列表指定的鉴别方式)
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#pppoe enable           (启动采用 PPP 会话的虚拟拨号接入方式)
```

```
Router(config-if)#exit
```

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.2 255.255.255.0
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.254 255.255.255.0
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#ip route 192.1.1.0 255.255.255.240 192.1.2.1
Router(config)#
```

5.3.2　局域网接入本地鉴别实验

1. 实验内容

(1) 完成本地鉴别配置。

(2) 完成局域网接入配置。

(3) 验证局域网接入过程。

2. 网络结构

局域网接入 Internet 过程如图 5.15 所示。对于接入控制设备 R1，边缘路由器等同于用户终端，同样通过 PPPoE 连接程序接入 Internet，因此，局域网接入下 R1 的配置和终端接入下 R1 的配置完全相同。对于内部网络终端，边缘路由器是互连内部网络和接入网络的路由器，通过端口地址转换(Port Address Translation，PAT)功能完成内部网络终端本地 IP 地址与边缘路由器连接接入网络接口的全球 IP 地址之间的转换，同时边缘

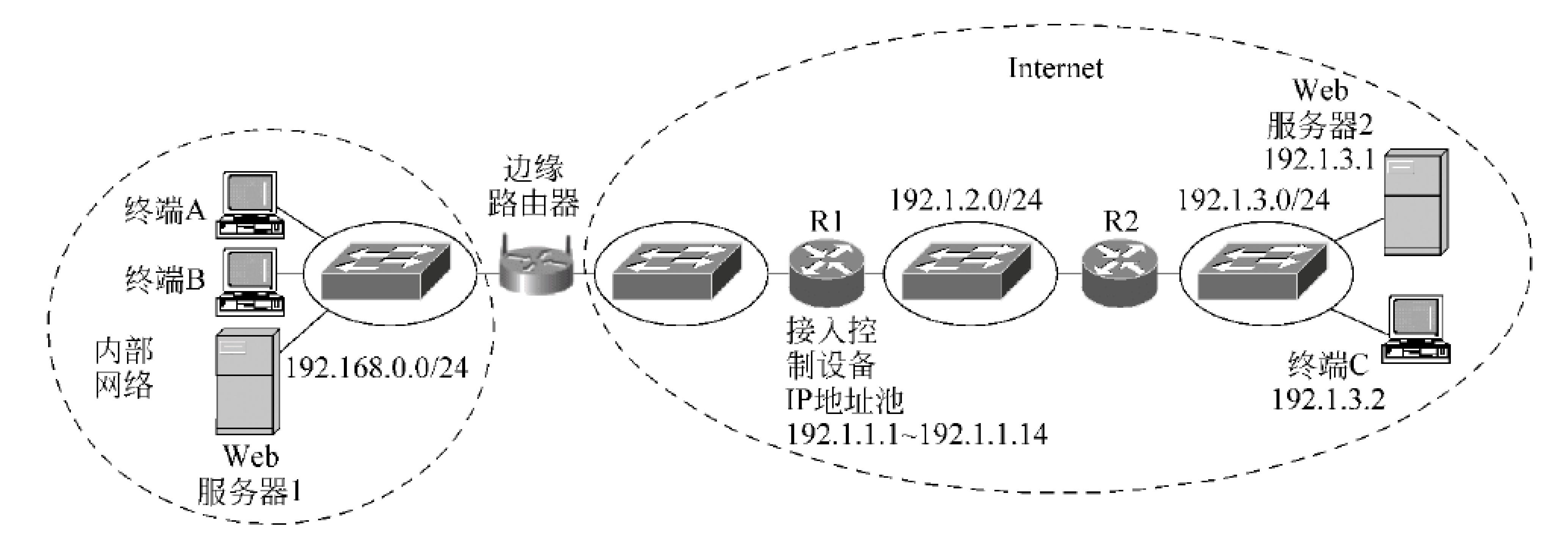


图 5.15　局域网接入 Internet 过程

路由器可以通过建立静态的端口和内部网络终端本地 IP 地址之间的映射，允许 Internet 终端发起访问内部网络服务器。

3. 实验步骤

（1）启动 Packet Tracer，在逻辑工作区根据图 5.15 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 5.16 所示。

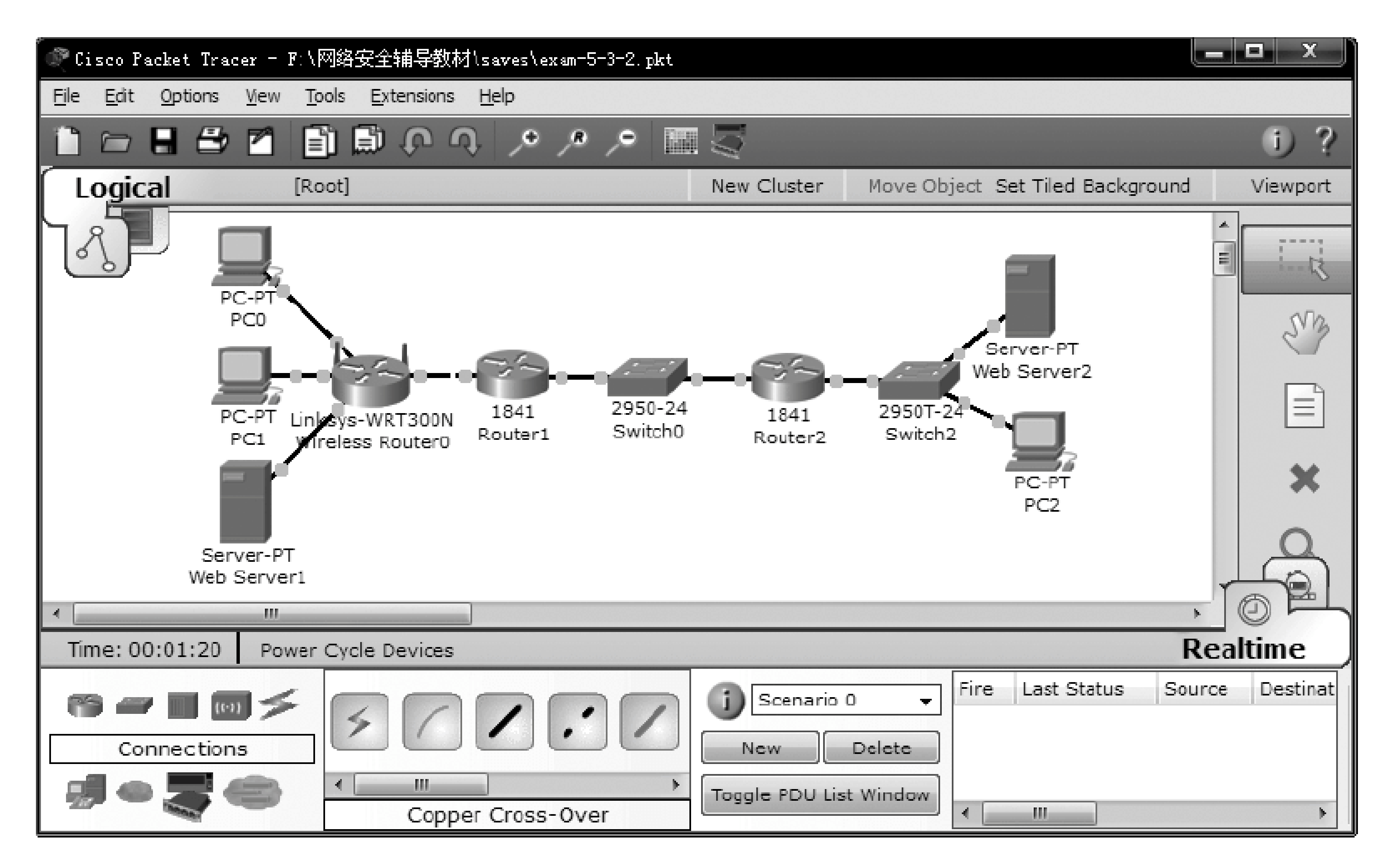


图 5.16　放置和连接设备后的逻辑工作区界面

（2）配置边缘路由器的 PPPoE 连接程序，配置界面如图 5.17 所示。输入用户名和口令，如<aaa1，bbb1>，PPPoE 连接程序定期发起连接过程，完成连接后，由接入控制设备 Router1 为边缘路由器分配全球 IP 地址，并在路由表中建立相应的路由项。边缘路由器接入 Internet 后，边缘路由器、Router1 和 Router2 的路由表如图 5.18～图 5.20 所示。

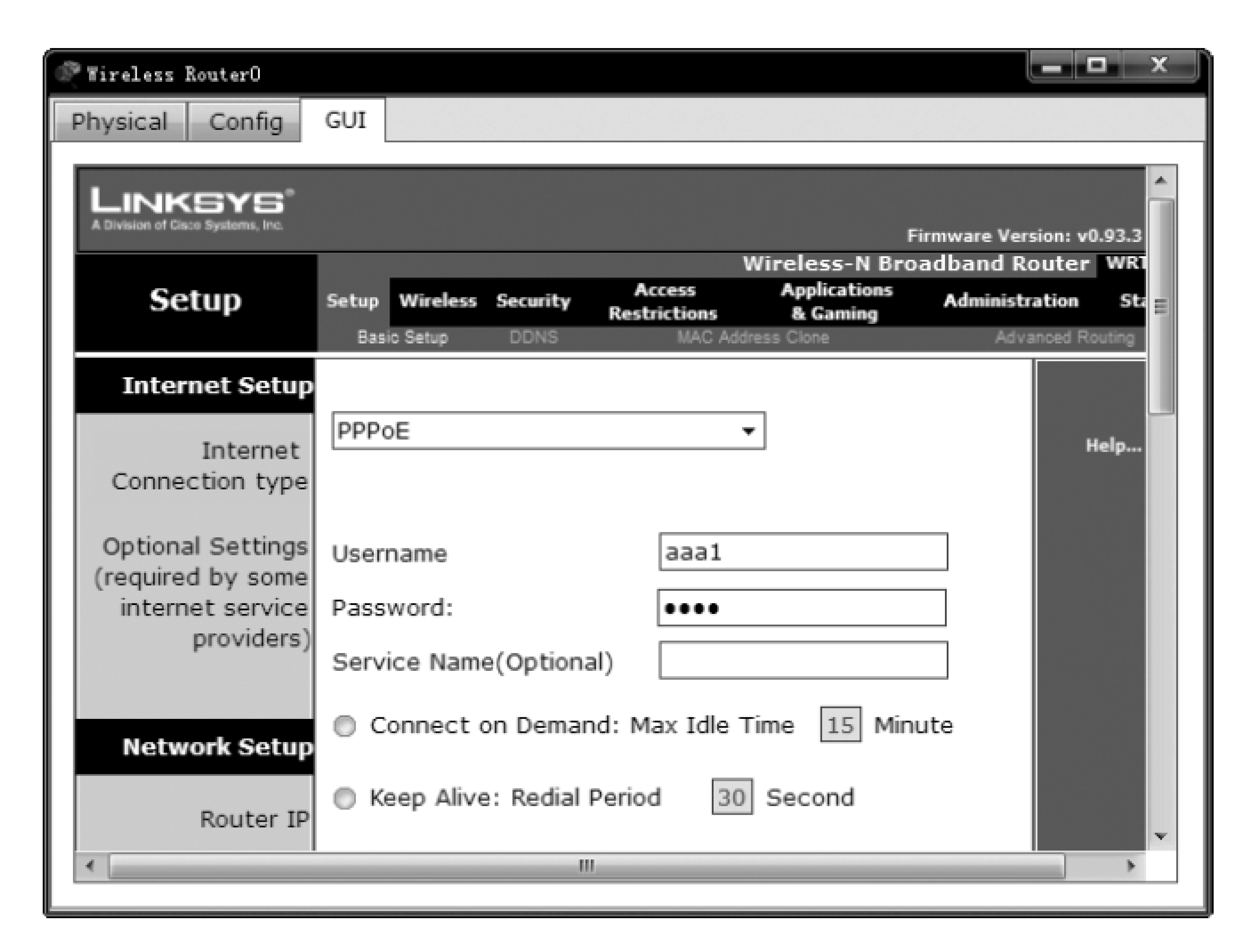


图 5.17　边缘路由器 PPPoE 配置界面

Routing Table for Wireless Router0

Type	Network	Port	Next Hop IP	Metric
C	192.1.1.1/32	Internet	---	0/0
C	192.168.0.0/24	Vlan1	---	0/0
S	0.0.0.0/0	---	1.1.1.1	1/0
S	1.1.1.1/32	Internet	---	1/0

图 5.18 接入 Internet 后边缘路由器路由表

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	1.0.0.0/8	FastEthernet0/0	---	0/0
C	192.1.1.1/32	Virtual-Access1.1	1.1.1.1	0/0
C	192.1.2.0/24	FastEthernet0/1	---	0/0
R	192.1.3.0/24	FastEthernet0/1	192.1.2.2	120/1

图 5.19 接入 Internet 后 Router1 路由表

Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet0/0	---	0/0
C	192.1.3.0/24	FastEthernet0/1	---	0/0
S	192.1.1.0/28	---	192.1.2.1	1/0

图 5.20 Router2 路由表

(3) 内部网络终端访问 Internet 时,使用 Router1 分配给边缘路由器的全球 IP 地址,同时需在 NAT 表中建立局域网内唯一源端口号与内部网络终端本地 IP 地址之间的映射。图 5.21 所示是 PC0 访问 Internet 中 Web Server2 的界面。内部网络终端 PC0 和 PC1 访问 Internet 中的 Web Server2 后,边缘路由器建立图 5.22 所示的 NAT 表,PC0 和 PC1 选择相同的源端口号 1025,边缘路由器为了用源端口号区分内部网络终端,分别用

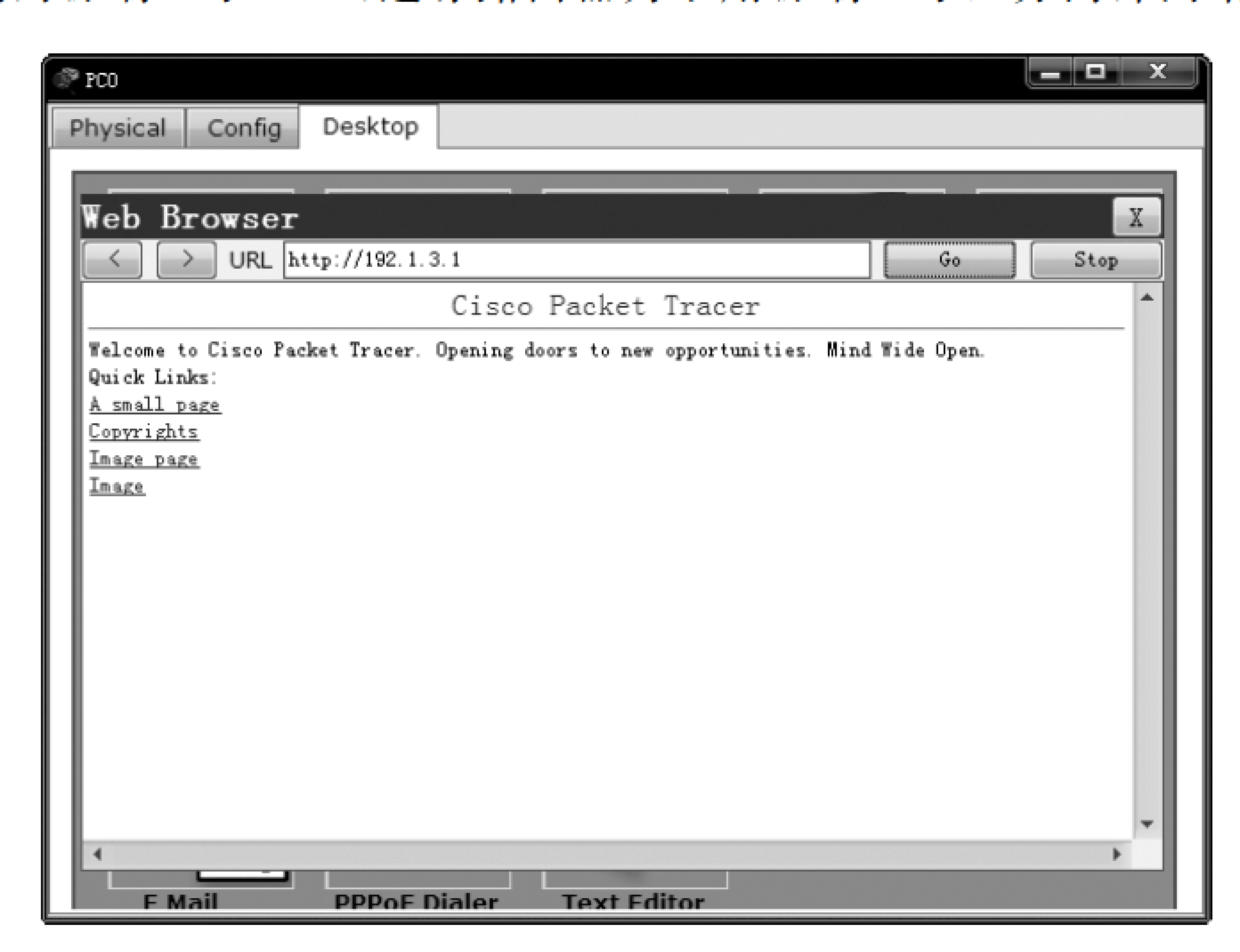


图 5.21 PC0 访问 Web Server2 的界面

NAT Table for Wireless Router0

Protocol	Inside Global	Inside Local	Outside Local	Outside Glol
tcp	192.1.1.1:1024	192.168.0.102:1025	192.1.3.1:80	192.1.3.1:80
tcp	192.1.1.1:1025	192.168.0.101:1025	192.1.3.1:80	192.1.3.1:80

图 5.22　边缘路由器 NAT 表

局域网内唯一的源端口 1024 和 1025 替换 PC0 和 PC1 的原始源端口号，并在 NAT 表中建立局域网内唯一的源端口号与 PC0 和 PC1 本地 IP 地址之间的映射。

(4) 图 5.15 所示网络结构中，只允许内部网络中的终端发起访问 Internet 中的终端和服务器，不允许 Internet 中的终端发起访问内部网络中的终端和服务器，但边缘路由器通过静态建立本地 IP 地址与局域网内唯一端口号之间的映射，可以允许 Internet 中的终端以该端口号为目的端口号、以 Router1 分配给边缘路由器的全球 IP 地址为目的 IP 地址发起访问内部网络终端和服务器。图 5.23 所示的配置界面将局域网内唯一的端口号 80 与内部网络终端的端口号 80 和内部网络本地 IP 地址 192.168.0.100 绑定在一起(局域网唯一端口号 80 和内部网络终端的端口号 80 由应用层协议 HTTP 指定)，边缘路由器只要接收到目的 IP 地址为 Router1 分配给边缘路由器的全球 IP 地址 192.1.1.1、目的端口号为 80 的 TCP 报文，将该 TCP 报文转发给本地 IP 地址为 192.168.0.100 的 Web Server1。图 5.24 所示是 PC2 通过输入 IP 地址 192.1.1.1 和端口号 80(端口号 80 由应用层协议 HTTP 指定)访问到 Web Server1 的界面。

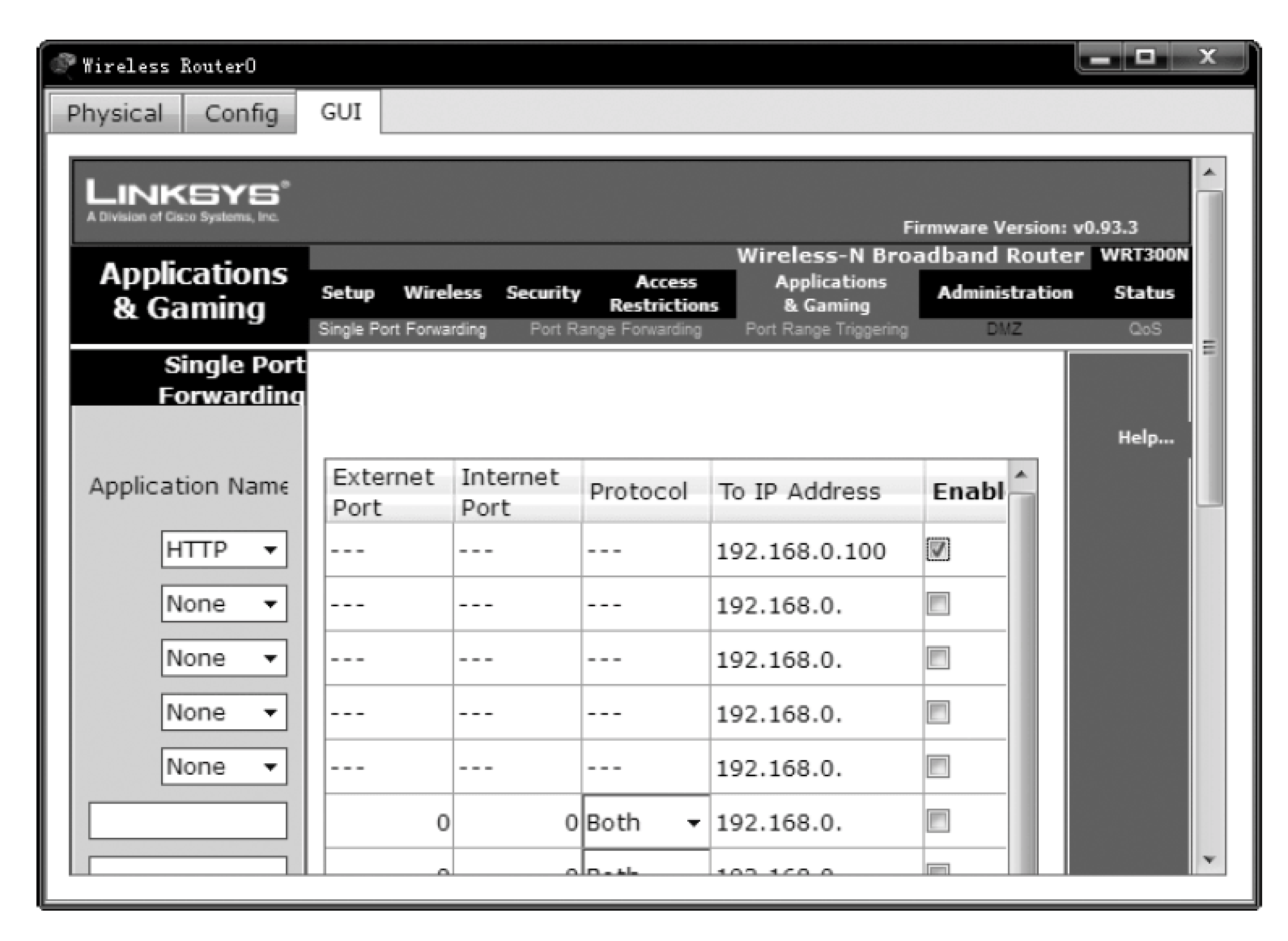


图 5.23　建立端口与内部终端本地地址之间的静态映射

(5) PC2 通过输入 IP 地址 192.1.1.1 和端口号 80 访问 Web Server1 后，边缘路由器的 NAT 表如图 5.25 所示，一项是将局域网内唯一的端口号 80 与内部网络终端的端口号 80 和内部网络本地 IP 地址 192.168.0.100 绑定在一起的静态映射，一项是 PC2 通过输入 IP 地址 192.1.1.1 和端口号 80 访问 Web Server1 建立的动态映射。

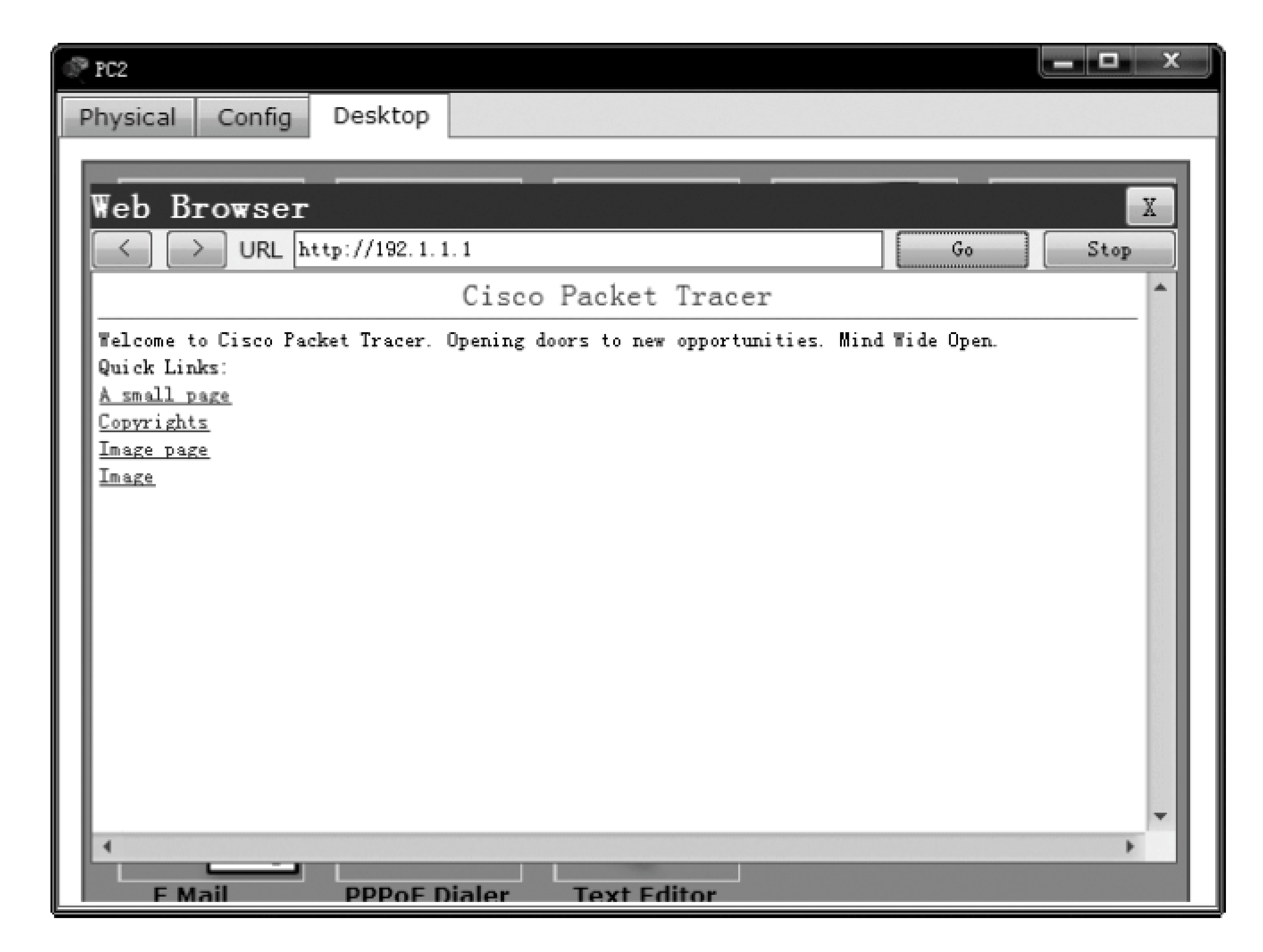
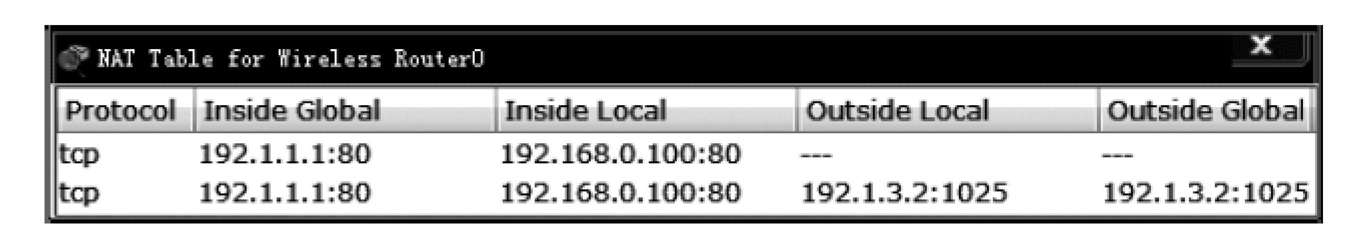


图 5.24　PC2 访问 Web Server1 的界面



NAT Table for Wireless Router0

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
tcp	192.1.1.1:80	192.168.0.100:80	---	---
tcp	192.1.1.1:80	192.168.0.100:80	192.1.3.2:1025	192.1.3.2:1025

图 5.25　内部终端地址与端口之间的静态映射

5.3.3　统一鉴别实验

1. 实验内容

(1) 完成网络配置。

(2) 完成统一鉴别下的接入控制设备配置。

(3) 完成 AAA 服务器配置。

(4) 验证统一鉴别下的接入过程。

2. 网络结构

本地鉴别机制需要在接入控制设备的本地用户库中创建所有允许通过该接入控制设备接入 Internet 的授权用户(用户名和口令),如果某个用户需要通过不同的接入控制设备接入 Internet,这些接入控制设备的本地用户库中都需创建该用户。这样做不仅麻烦,而且不利于统一管理,因此,实际应用中配置统一的鉴别服务器——AAA 服务器,接入控制设备接收到用户的身份鉴别请求后,向鉴别服务器转发该身份鉴别请求。由于接入控制设备和鉴别服务器之间通过公共网络互连,因此需要将用户提供的鉴别信息加密后传输给鉴别服务器。接入控制设备需配置鉴别服务器地址和加密用户鉴别信息的共享密钥,每一个接入控制设备可以采用不同的共享密钥。鉴别服务器中统一创建允许接入 Internet 的所有授权用户,因此,授权用户可以通过任意接入控制设备接入 Internet。

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 5.26 所示的网络结构放置和连接设

备，完成设备放置和连接后的逻辑工作区界面如图 5.27 所示。

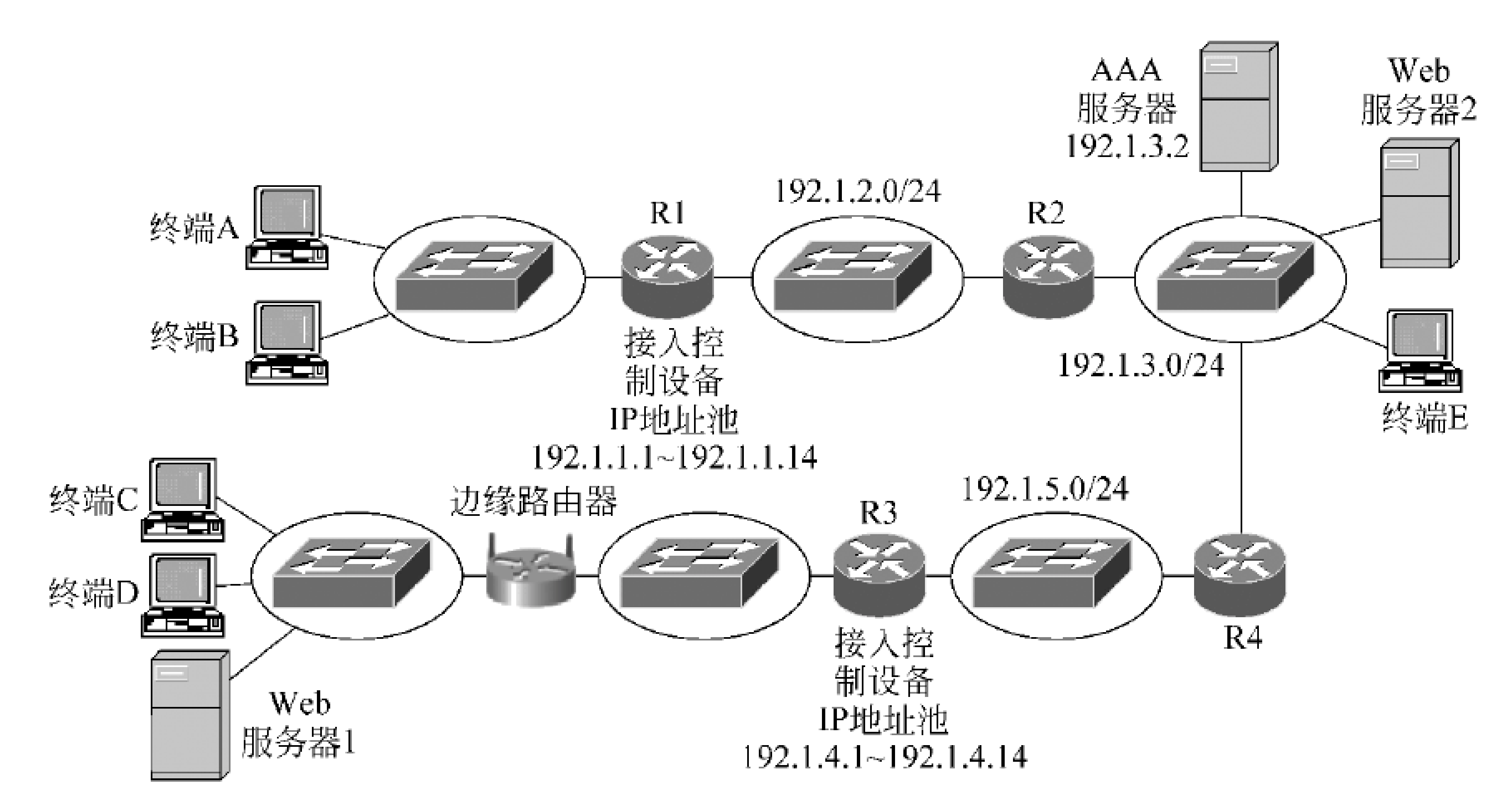


图 5.26 统一鉴别下的 Internet 接入过程

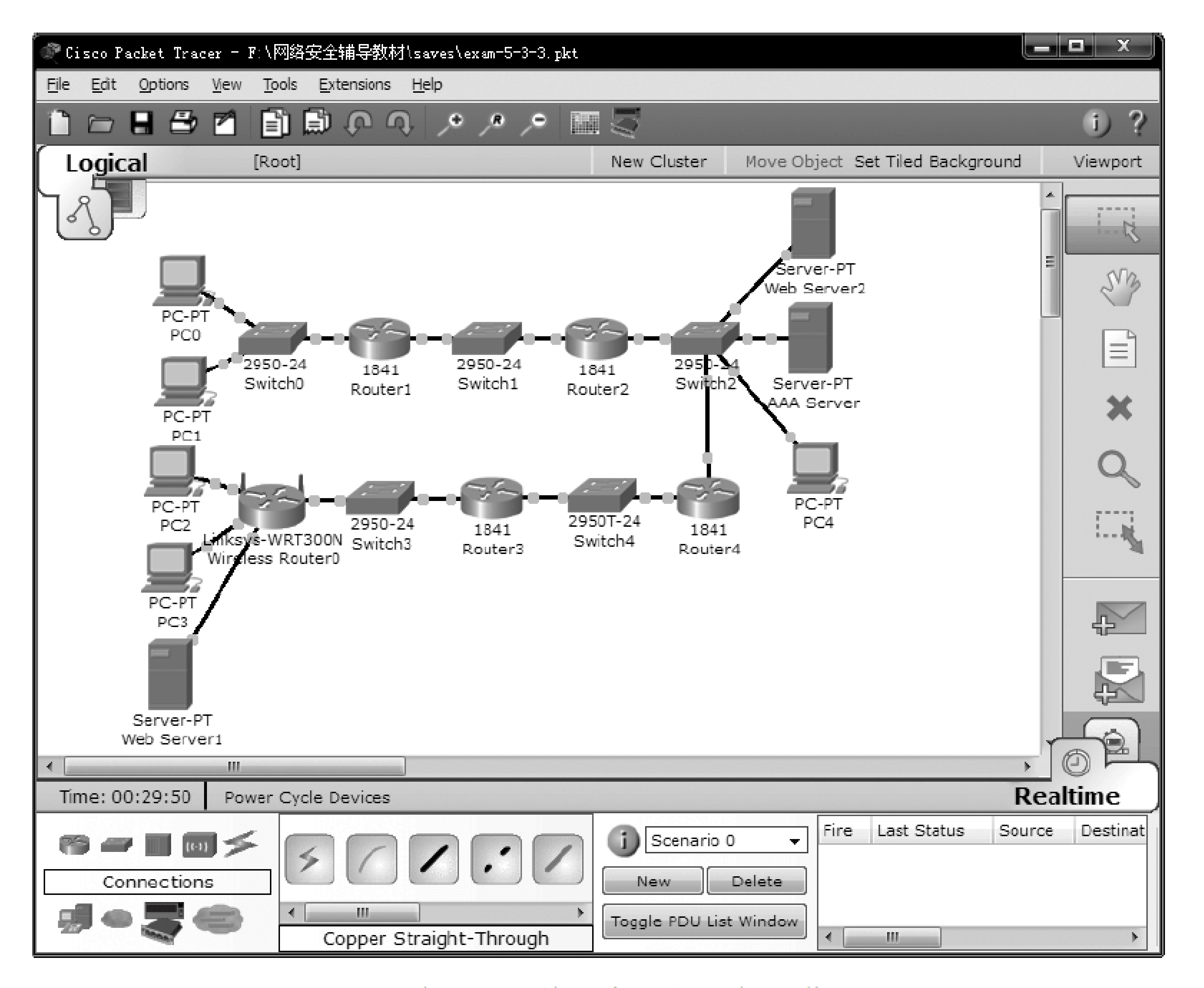


图 5.27 放置和连接设备后的逻辑工作区界面

（2）完成路由器接口 IP 地址和子网掩码配置，完成各个路由器路由协议配置和静态路由项配置。需要指出的是，除了 RIP 生成的动态路由项外，各个路由器还需配置用于指明通往网络 192.1.1.0/28 和 192.1.4.0/27 传输路径的静态路由项。各个路由器生成的路由表如图 5.28～图 5.31 所示。

（3）完成鉴别服务器配置。图 5.32 所示是鉴别服务器配置界面，需要配置两部分内

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	1.0.0.0/8	FastEthernet0/0	---	0/0
C	192.1.2.0/24	FastEthernet0/1	---	0/0
R	192.1.3.0/24	FastEthernet0/1	192.1.2.253	120/1
R	192.1.5.0/24	FastEthernet0/1	192.1.2.253	120/2
S	192.1.4.0/28	---	192.1.2.253	1/0

图 5.28 终端接入 Internet 前的 Router1 路由表

Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet0/0	---	0/0
C	192.1.3.0/24	FastEthernet0/1	---	0/0
R	192.1.5.0/24	FastEthernet0/1	192.1.3.253	120/1
S	192.1.1.0/28	---	192.1.2.254	1/0
S	192.1.4.0/28	---	192.1.3.253	1/0

图 5.29 Router2 路由表

Routing Table for Router3

Type	Network	Port	Next Hop IP	Metric
C	192.1.5.0/24	FastEthernet0/1	---	0/0
C	2.0.0.0/8	FastEthernet0/0	---	0/0
R	192.1.2.0/24	FastEthernet0/1	192.1.5.253	120/2
R	192.1.3.0/24	FastEthernet0/1	192.1.5.253	120/1
S	192.1.1.0/28	---	192.1.5.253	1/0

图 5.30 边缘路由器接入 Internet 前的 Router3 路由表

Routing Table for Router4

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	FastEthernet0/1	---	0/0
C	192.1.5.0/24	FastEthernet0/0	---	0/0
R	192.1.2.0/24	FastEthernet0/1	192.1.3.254	120/1
S	192.1.1.0/28	---	192.1.3.254	1/0
S	192.1.4.0/28	---	192.1.5.254	1/0

图 5.31 Router4 路由表

容：一是配置作为网络接入服务器(Network Access Server，NAS)的 Router1 和 Router3 的相关信息，客户端名字(ClientName)在 Router1 和 Router3 中通过命令“hostname router”确定，客户端 IP 地址(ClientIP)是 Router1 和 Router3 向 AAA 服务器发送 RADIUS 报文时，用于输出 RADIUS 报文的接口的 IP 地址。密钥(secret)在 Router1 和 Router3 中分别通过命令“radius-server key router1”和“radius-server key router3”确定。二是配置授权用户信息，这里配置了三个授权用户的用户名和口令。

(4) 完成 Router1 和 Router3 与接入控制相关的配置。与 5.3.1 节终端接入本地鉴别实验不同的是，由鉴别服务器统一鉴别，因此需要通过命令“aaa authentication ppp a1 group radius” 定义名为 a1 的鉴别列表，该鉴别列表确定 PPP 鉴别用户身份时统一使用 RADIUS 鉴别服务器中配置的用户信息，因此需要通过命令“radius-server host 192.1.3.2”指定 RADIUS 鉴别服务器 IP 地址 192.1.3.2，通过命令“radius-server key router1”指定 router1 为 Router1 与 RADIUS 鉴别服务器的共享密钥，RADIUS 鉴别服务器通过

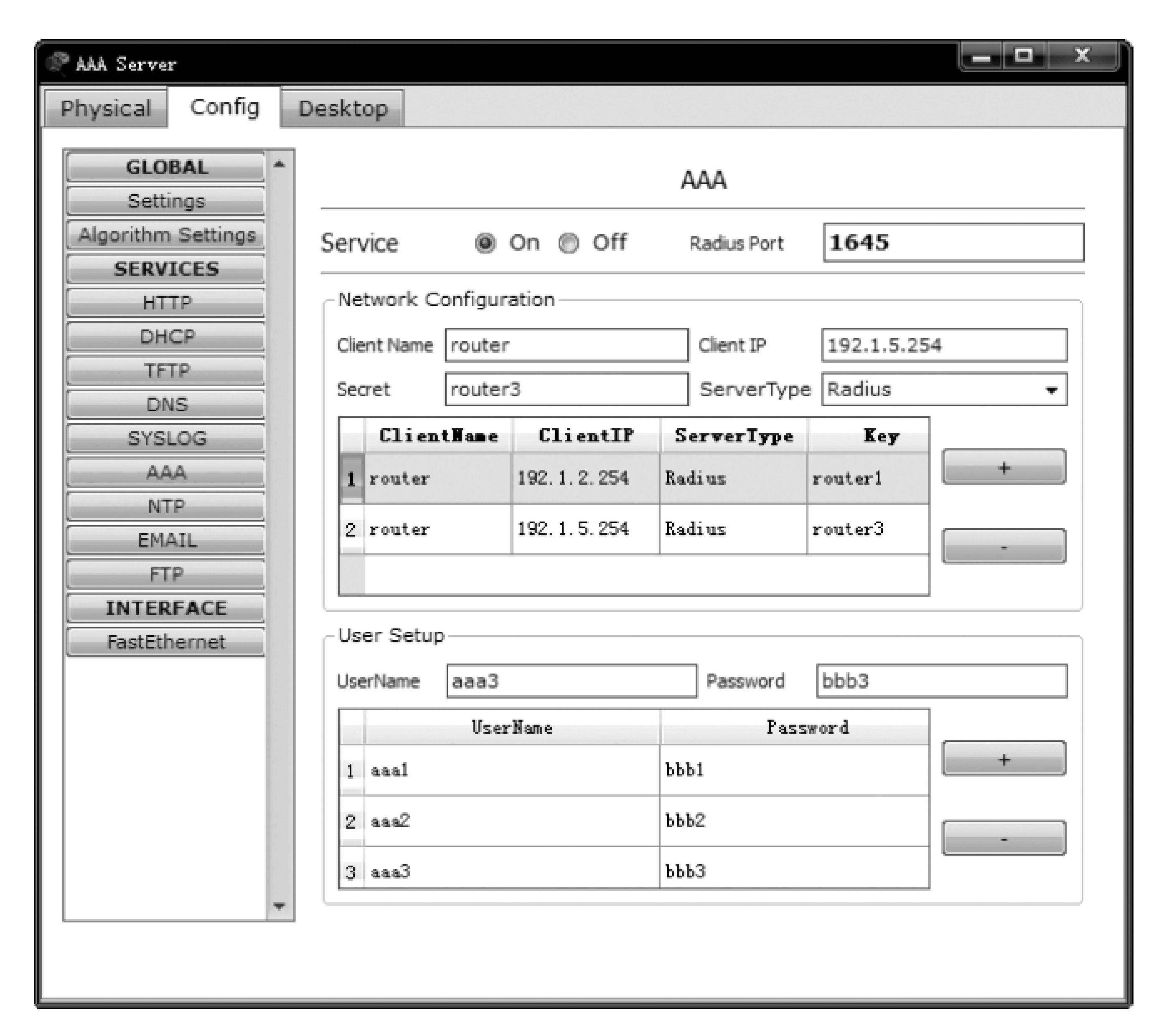


图 5.32 AAA 服务器配置界面

共享密钥鉴别 Router1 身份，Router1 通过共享密钥加密传输给 RADIUS 鉴别服务器的机密信息，如口令等。Router3 通过命令“radius-server key router3”指定 router3 为 Router3 与 RADIUS 鉴别服务器的共享密钥。

（5）完成 Router1 和 Router3 与接入控制相关的配置后，边缘路由器可以启动 PPPoE 连接程序，连接程序配置界面如图 5.33 所示，边缘路由器定期启动 PPPoE 连接过程。边缘路由器接入 Internet 后的边缘路由器路由表如图 5.34 所示，Router3 路由表

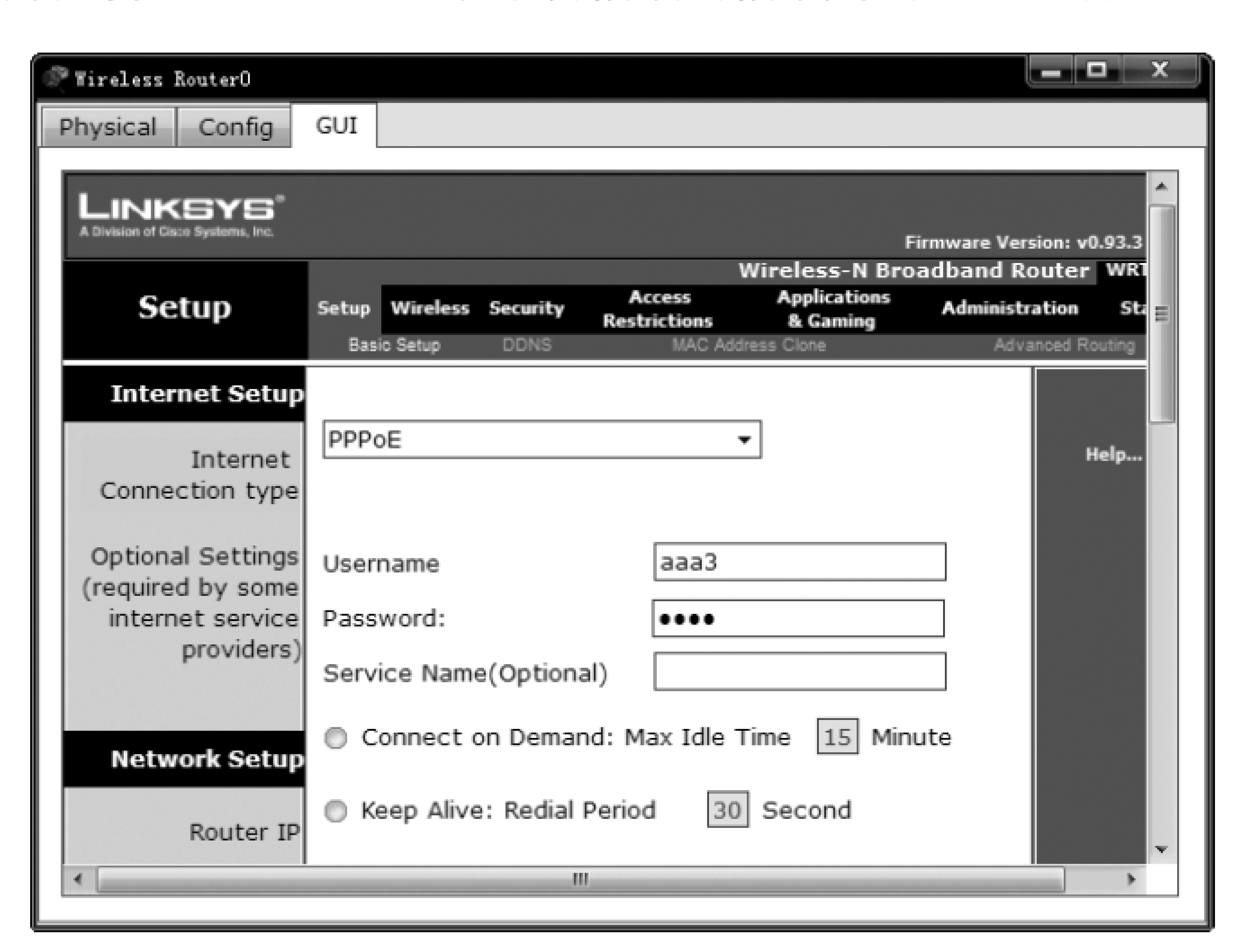


图 5.33 边缘路由器 PPPoE 连接程序配置界面

如图 5.35 所示。终端同样可以通过 PPPoE 连接程序接入 Internet，PC0 PPPoE 连接程序界面如图 5.36 所示，终端接入 Internet 后的 Router1 路由表如图 5.37 所示。

Routing Table for Wireless Router0

Type	Network	Port	Next Hop IP	Metric
C	192.1.4.1/32	Internet	---	0/0
C	192.168.0.0/24	Vlan1	---	0/0
S	0.0.0.0/0	---	2.2.2.2	1/0
S	2.2.2.2/32	Internet	---	1/0

图 5.34　接入 Internet 后的边缘路由器路由表

Routing Table for Router3

Type	Network	Port	Next Hop IP	Metric
C	192.1.4.1/32	Virtual-Access1.1	2.2.2.2	0/0
C	192.1.5.0/24	FastEthernet0/1	---	0/0
C	2.0.0.0/8	FastEthernet0/0	---	0/0
R	192.1.2.0/24	FastEthernet0/1	192.1.5.253	120/2
R	192.1.3.0/24	FastEthernet0/1	192.1.5.253	120/1
S	192.1.1.0/28	---	192.1.5.253	1/0

图 5.35　边缘路由器接入 Internet 后的 Router3 路由表



图 5.36　PC0 PPPoE 连接程序界面

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	1.0.0.0/8	FastEthernet0/0	---	0/0
C	192.1.1.1/32	Virtual-Access1.1	1.1.1.1	0/0
C	192.1.1.2/32	Virtual-Access1.2	1.1.1.1	0/0
C	192.1.2.0/24	FastEthernet0/1	---	0/0
R	192.1.3.0/24	FastEthernet0/1	192.1.2.253	120/1
R	192.1.5.0/24	FastEthernet0/1	192.1.2.253	120/2
S	192.1.4.0/28	---	192.1.2.253	1/0

图 5.37　终端接入 Internet 后的 Router1 路由表

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 1.1.1.1 255.0.0.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#exit
Router(config)#ip route 192.1.4.0 255.255.255.240 192.1.2.253
Router(config)#aaa new-model
Router(config)#aaa authentication ppp a1 group radius
                    (定义名为 a1 的鉴别列表,该鉴别列表确定 PPP 鉴别用户
                     身份时统一使用 RADIUS 鉴别服务器中配置的用户信息)
Router(config)#radius-server host 192.1.3.2
                    (指定 RADIUS 鉴别服务器 IP 地址 192.1.3.2)
Router(config)#radius-server key router1
                    (指定 Router1 与 RADIUS 鉴别服务器的共享密钥为 router1)
Router(config)#hostname router      (确定客户端名字为 router)
Router(config)#vpdn enable
Router(config)#vpdn-group b1
Router(config-vpdn)#accept-dialin
Router(config-vpdn-acc-in)#protocol pppoe
Router(config-vpdn-acc-in)#exit
Router(config-vpdn)#exit
Router(config)#ip local pool c1 192.1.1.1 192.1.1.14
Router(config)#interface virtual-template 1
Router(config-if)#ip unnumbered FastEthernet0/0
Router(config-if)#peer default ip address pool c1
Router(config-if)#ppp authentication chap a1
                    (按照名为 a1 的鉴别列表要求鉴别接入用户身份)
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#pppoe enable
Router(config-if)#exit
```

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.253 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#ip route 192.1.1.0 255.255.255.240 192.1.2.254
Router(config)#ip route 192.1.4.0 255.255.255.240 192.1.3.253
Router(config)#
```

（3）Router3 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 2.2.2.2 255.0.0.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.5.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.5.0
Router(config-router)#exit
Router(config)#ip route 192.1.1.0 255.255.255.240 192.1.5.253
Router(config)#aaa new-model
Router(config)#aaa authentication ppp a1 group radius
Router(config)#radius-server host 192.1.3.2
Router(config)#radius-server key router3
                    (指定 Router3 与 RADIUS 鉴别服务器的共享密钥为 router3)
Router(config)#hostname router
Router(config)#vpdn enable
Router(config)#vpdn-group b1
Router(config-vpdn)#accept-dialin
Router(config-vpdn-acc-in)#protocol pppoe
```

```
Router(config-vpdn-acc-in)#virtual-template 1
Router(config-vpdn-acc-in)#exit
Router(config-vpdn)#exit
Router(config)#ip local pool c1 192.1.4.1 192.1.4.14
Router(config)#interface virtual-template 1
Router(config-if)#ip unnumbered FastEthernet0/0
Router(config-if)#peer default ip address pool c1
Router(config-if)#ppp authentication chap a1
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#pppoe enable
Router(config-if)#exit
Router(config)#
```

(4) Router4 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.5.253 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.253 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.5.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#ip route 192.1.1.0 255.255.255.240 192.1.3.254
Router(config)#ip route 192.1.4.0 255.255.255.240 192.1.5.254
Router(config)#
```

5.3.4 综合统一鉴别实验

1. 实验内容

(1) 完成网络配置。
(2) 完成统一鉴别下的接入控制设备配置。
(3) 完成统一鉴别下的路由器远程登录配置。
(4) 完成 AAA 服务器配置。
(5) 验证统一鉴别下的接入过程。
(6) 验证统一鉴别下的远程登录过程。

2. 网络结构

网络结构如图 5.9 所示。R1、R3 和 R5 为接入控制设备，R1 控制终端经过以太网接入 Internet 的接入过程，R3 控制局域网通过边缘路由器接入 Internet 的接入过程，R5 控制终端经过 ADSL 接入 Internet 的接入过程。图中的 AAA 服务器为 RADIUS 鉴别服务器，接入鉴别过程中，R1、R3 和 R5 作为网络接入服务器向 AAA 服务器转发用户的鉴别信息，统一由 AAA 服务器完成对接入用户的身份鉴别。除了接入用户身份鉴别外，由 AAA 服务器统一完成对实施路由器远程配置的管理员的身份鉴别。因此，AAA 服务器同时承担对接入用户和远程配置路由器的设备管理人员的身份鉴别功能，这是称 AAA 服务器为综合鉴别服务器的原因。

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 5.9 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 5.38 所示。图中 ADSL 路由器的 FastEthernet 接口连接 PC4 的 FastEthernet 接口，用户线接口通过电话线连接 DSLAM，这里用 WAN 仿真设备仿真 DSLAM，因此通过图 5.39 所示配置界面将用户线接口与 FastEthernet 接口绑定在一起。

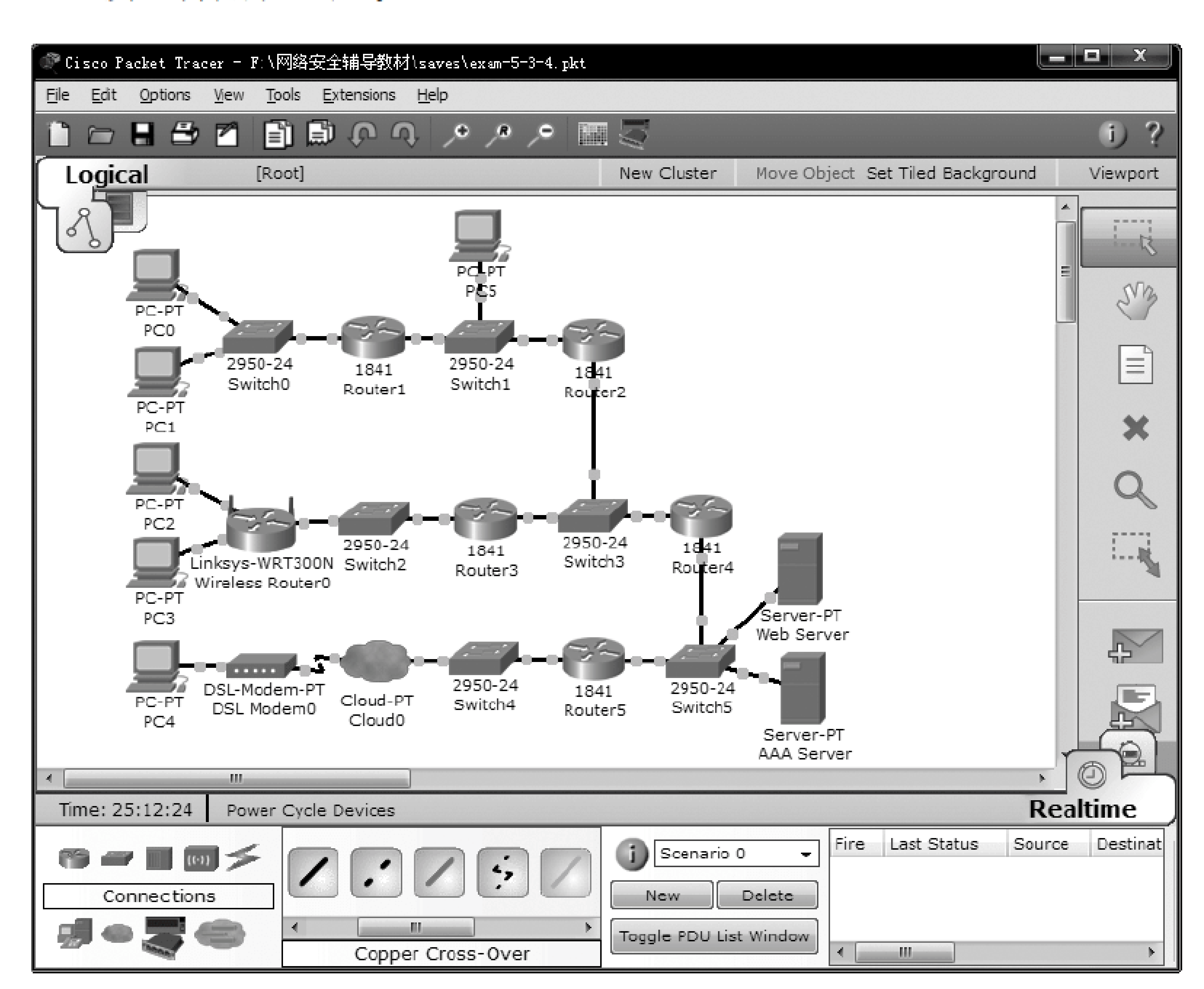


图 5.38　放置和连接设备后的逻辑工作区界面

(2) 完成路由器接口 IP 地址和子网掩码配置、动态路由协议配置和静态路由项配置，各个路由器生成路由表。

(3) 完成 R1、R3 和 R5 与接入控制相关的配置，同时完成各个路由器与远程登录相关的配置，Router5 中通过命令“aaa authentication login a2 group radius”定义名为 a2 的

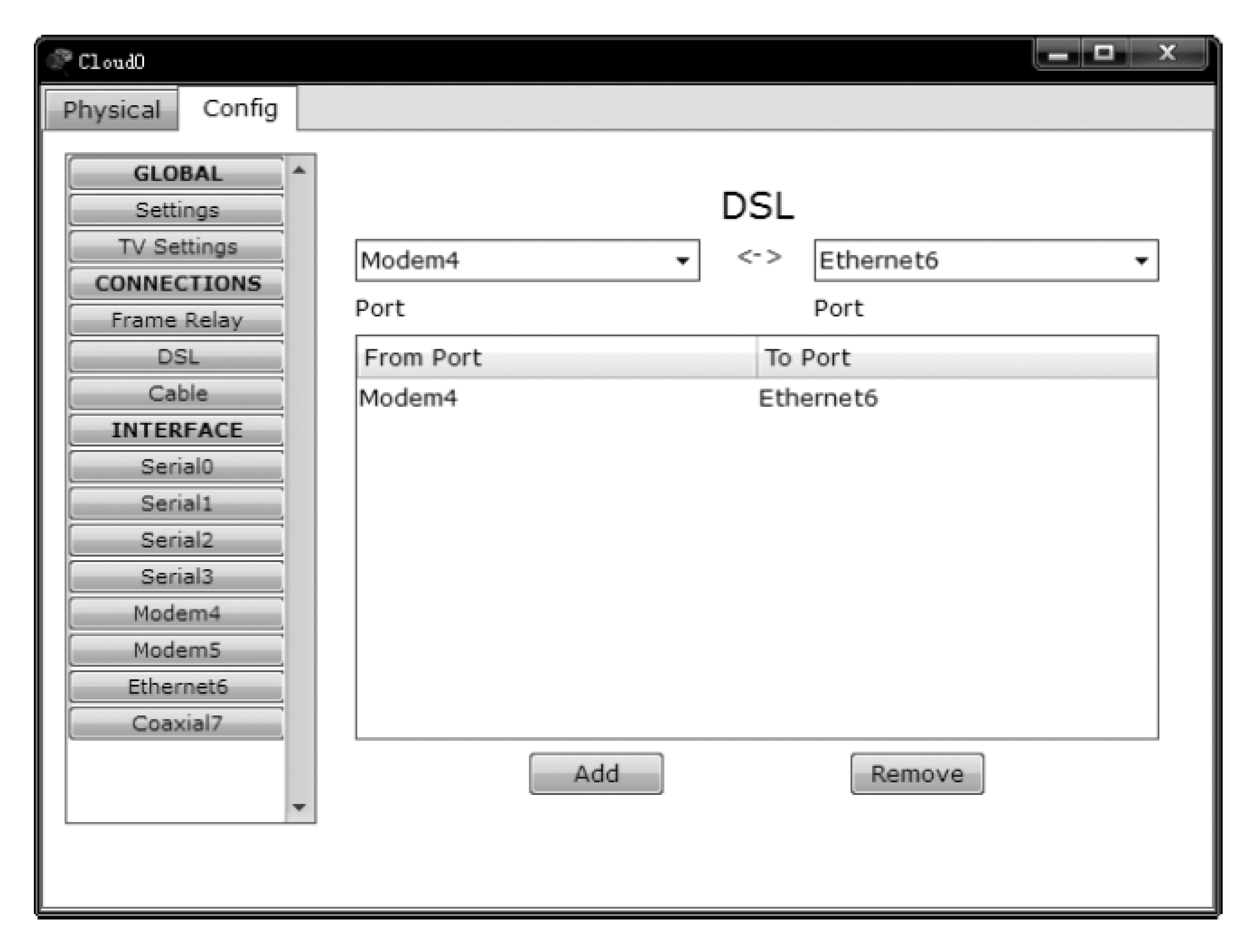


图 5.39 仿真 DSLAM 设备将用户线和以太网绑定在一起的界面

鉴别列表，该鉴别列表确定统一使用 RADIUS 鉴别服务器中配置的用户信息鉴别远程登录用户身份。在虚拟端口配置模式通过命令“login authentication a2”指定根据名为 a2 的鉴别列表的要求鉴别远程登录用户身份。

(4) 完成 AAA 服务器配置。图 5.40 给出了作为 NAS 的路由器 Router1、Router3 和 Router5 的相关配置和三个授权用户的相关配置，如果所有路由器都需实施远程配置，这些路由器都应作为 NAS 在 AAA 服务器中完成相关配置。

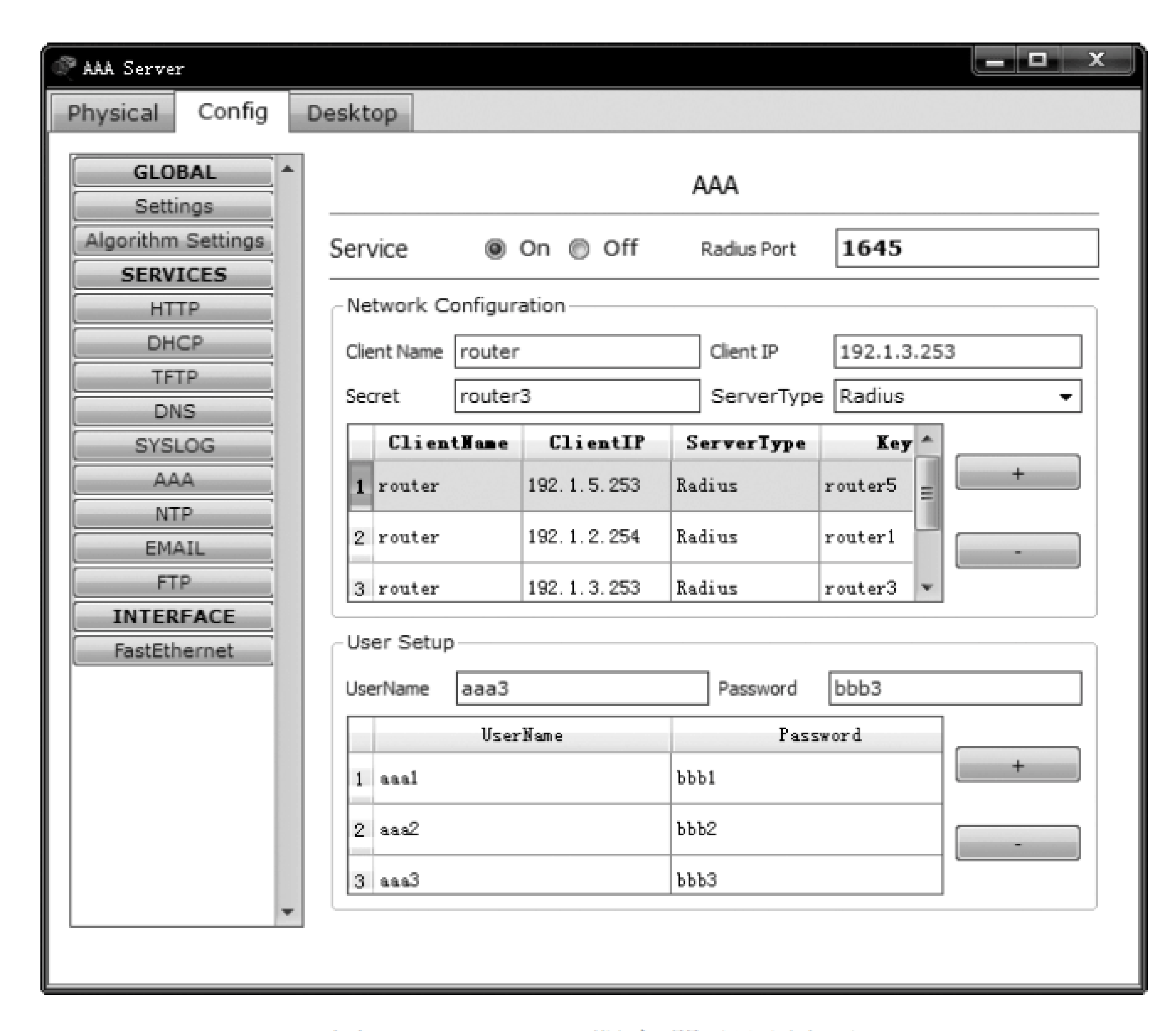


图 5.40 AAA 服务器配置界面

(5) 完成 Router5 有关接入控制配置和 AAA 服务器的相关配置。PC4 可以通过启动 PPPoE 连接程序接入 Internet，启动 PPPoE 连接程序时需输入 AAA 服务器配置的授权用户信息，如图 5.41 所示。PC4 接入 Internet 后的 Router5 路由表如图 5.42 所示。



图 5.41　PC4 PPPoE 连接程序界面

Routing Table for Router5

Type	Network	Port	Next Hop IP	Metric
C	192.1.5.0/24	FastEthernet0/1	---	0/0
C	192.1.6.1/32	Virtual-Access1.1	3.3.3.3	0/0
C	3.0.0.0/8	FastEthernet0/0	---	0/0
R	192.1.2.0/24	FastEthernet0/1	192.1.5.254	120/2
R	192.1.3.0/24	FastEthernet0/1	192.1.5.254	120/1
S	192.1.1.0/28	---	192.1.5.254	1/0
S	192.1.4.0/28	---	192.1.5.254	1/0

图 5.42　终端接入 Internet 后的 Router5 路由表

(6) PC4 接入 Internet 后，可以访问 Internet 中的资源。图 5.43 所示是 PC4 访问 Web 服务器的界面。

(7) PC5 可以实施对路由器的远程配置。图 5.44 所示是 PC5 远程配置 Router5 的界面，需要输入的用户信息必须是 AAA 服务器配置的授权用户信息。

4. 命令行配置过程

Router5 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 3.3.3.3 255.0.0.0
Router(config-if)#exit
```

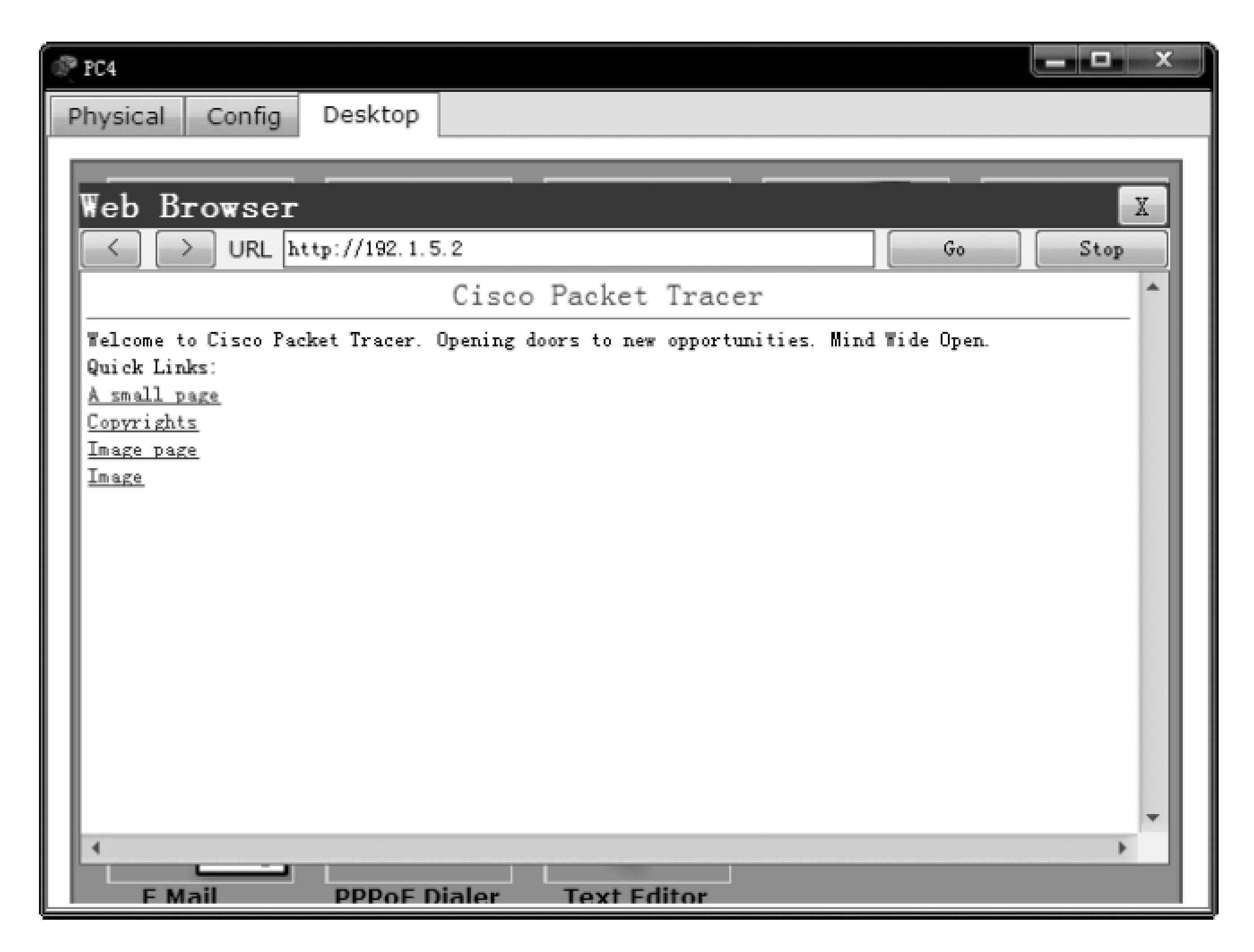


图 5.43 PC4 访问 Web Server 的界面

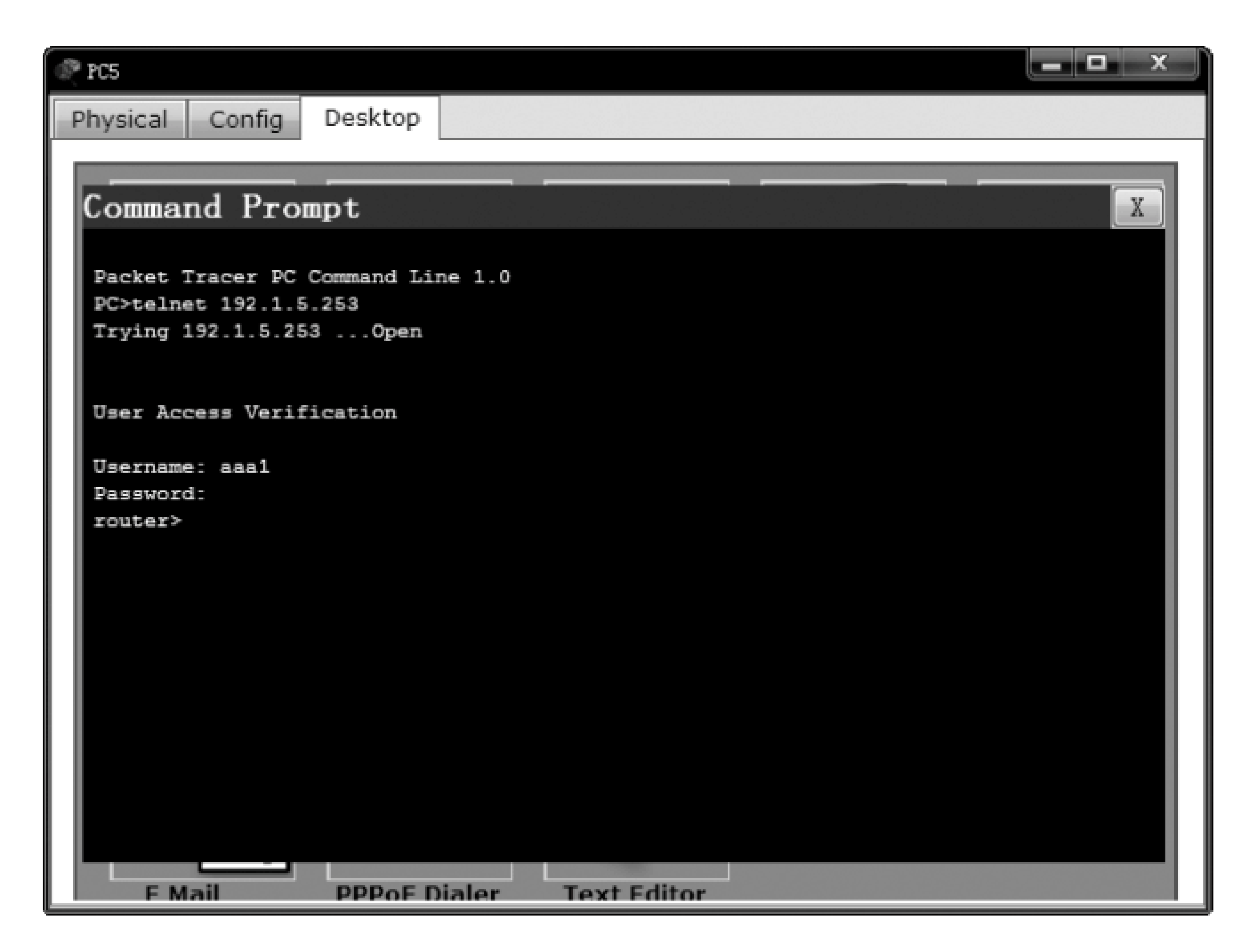


图 5.44 PC5 远程登录 Router5 界面

```
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.5.253 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.5.0
Router(config-router)#exit
Router(config)#ip route 192.1.1.0 255.255.255.240 192.1.5.254
Router(config)#ip route 192.1.4.0 255.255.255.240 192.1.5.254
Router(config)#aaa new-model
```

```
Router(config)#aaa authentication ppp a1 group radius
Router(config)#aaa authentication login a2 group radius
                              (定义名为 a2 的鉴别列表。该鉴别列表确定统一使用 RADIUS
                               鉴别服务器中配置的用户信息鉴别远程登录用户身份)
Router(config)#radius-server host 192.1.5.1
router(config)#radius-server key router5
Router(config)#hostname router
router(config)#vpdn enable
router(config)#vpdn-group b1
router(config-vpdn)#accept-dialin
router(config-vpdn-acc-in)#protocol pppoe
router(config-vpdn-acc-in)#virtual-template 1
router(config-vpdn-acc-in)#exit
router(config-vpdn)#exit
router(config)#ip local pool c1 192.1.6.1 192.1.6.14
router(config)#interface virtual-template 1
router(config-if)#ip unnumbered FastEthernet0/0
router(config-if)#peer default ip address pool c1
router(config-if)#ppp authentication chap a1
                               (按照名为 a1 的鉴别列表要求鉴别接入用户身份)
router(config-if)#exit
router(config)#interface FastEthernet0/0
router(config-if)#pppoe enable
router(config-if)#exit
router(config)#access-list 1 permit host 192.1.2.1
                        (配置只处理源 IP 地址为 192.1.2.1 的 IP 分组的标准访问控制列表)
router(config)#access-list 1 deny any
router(config)#line vty 0 15
router(config-line)#login authentication a2
                               (按照名为 a2 的鉴别列表要求鉴别远程登录用户身份)
router(config-line)#access-class 1 in
                               (通过编号为 1 的标准访问列表指定允许远程配置的终端)
router(config-line)#exit
router(config)#
```

其他路由器的命令行配置过程或是 Router5 的子集，都与 Router5 相似，不再赘述。

第 6 章 网络安全技术

CHAPTER

6.1 知识要点

6.1.1 网络设备和安全设备

网络设备是指用于实现数据端到端传输的设备，包括实现同一网络内两个结点之间数据传输的设备，如以太网交换机、集线器等，以及实现因特网内数据端到端传输的设备，如路由器等。安全设备是指专职用于实现网络安全功能的设备，如专职防火墙、网络入侵防御系统和主机入侵防御系统等。

目前的趋势是设备融合，网络设备中嵌入安全功能，安全设备中嵌入数据传输功能，但基本上还是把嵌入安全功能的交换机、路由器等称为网络设备，因为它们的主要功能是实现数据传输。

网络安全技术主要讨论嵌入在网络设备中的安全技术。由于许多安全功能必须在数据传输过程中的某个环节予以实现，因此，网络设备提供的安全功能是安全设备无法代替的。

6.1.2 以太网安全功能

1. 接入控制

终端接入网络的主要途径有两个：一是通过接入网络，如 ADSL、PSTN 等；二是通过局域网，如以太网、无线局域网等。对于采用接入网络途径的终端，由于存在接入控制过程，保证只有授权终端接入网络。对于采用局域网途径的终端，必须增加接入控制机制，如配置以太网交换机端口的访问控制列表、使用以太网交换机端口接入控制协议 802.1X 等。

以太网接入控制的主要任务有两个：一是保证只有授权终端接入网络；二是禁止终端冒用其他终端的 IP 地址和 MAC 地址。

2. 信任端口

DHCP 欺骗攻击的危害很大，且难以预防，以太网必须禁止伪造的 DHCP 服务器接入，当然，判定某个接入主机是否是 DHCP 服务器是比较

困难的,解决机制是禁止未经允许的服务器发送 DHCP 响应报文。

以太网交换机端口可以配置为信任端口和非信任端口,只有从信任端口接收到的 DHCP 响应报文,如提供报文和确认报文才能继续转发,所有从非信任端口接收到的 DHCP 响应报文一律丢弃。只有直接连接 DHCP 服务器的端口和用于互连交换机的端口才被配置成信任端口,其他端口一律配置为非信任端口。这样,只有从连接信任端口的 DHCP 服务器发送的响应报文才能到达终端,其他伪造的 DHCP 服务器发送的响应报文都被以太网交换机丢弃。

3. VLAN

VLAN 划分的原始作用是缩小广播域,降低广播造成的带宽浪费。VLAN 安全方面的作用有三个:一是由于每一个 VLAN 是逻辑上独立的以太网,而许多攻击手段都是针对同一网络中的终端,如 ARP 欺骗攻击,因此 VLAN 划分可以有效缩小黑客攻击范围。二是通过将具有不同安全等级的信息资源放入不同的 VLAN,同时通过设置防火墙的访问控制策略对 VLAN 间的信息传输过程实施控制,可以防止黑客对重要信息资源的非法访问。三是许多厂家的二层交换机都是将默认 VLAN——VALN 1 作为管理 VLAN,通过将 VLAN 1 完全独立出来,只允许 VLAN 1 内的终端配置和管理二层交换机,可以有效提高设备管理的安全性。

6.1.3 安全路由功能

路由项欺骗攻击是目前常见的信息截获手段,通过改变 IP 分组端到端传输路径,使 IP 分组经过黑客终端,从而使黑客终端能够截获经过它的 IP 分组。决定 IP 层传输路径的是路由表,路由器通过相互之间交换路由协议报文得出各项路由项。安全路由功能就是保证路由器只处理授权路由器发送的、且没有被篡改的路由协议报文。这就要求路由器对接收到的路由协议报文进行源端鉴别,并进行完整性检测。实现这一功能需要为所有授权路由器配置相同的共享密钥,而且所有路由器发送的路由协议报文必须附加基于共享密钥和 HMAC 算法计算所得的消息鉴别码,使得接收端可以通过消息鉴别码实现源端鉴别和完整性检测。

6.1.4 内部网络隐藏功能

无分类编址和 NAT 是解决 IPv4 地址短缺的有效手段,但 NAT 隐藏内部网络的功能,同时又增强了内部网络的安全性。除非黑客连接在内部网络上,否则内部网络对于黑客是透明的,黑客无法对内部网络中的终端发起主动攻击。内部网络使用本地 IP 地址,即私有地址,同时使公共网络(或外部网络)路由器中的路由表不存在以内部网络本地 IP 地址为目的网络地址的路由项。在互连内部网络和公共网络的边缘路由器中建立内部网络本地 IP 地址与全球 IP 地址之间映射前,内部网络和公共网络之间不能通信。内部网络本地 IP 地址与全球 IP 地址之间映射或者通过配置静态建立,或者由内部网络中的终端发起建立。

6.1.5　网络容错功能

容错指的是一种在网络中的一些物理链路和一些转发结点(如交换机、路由器)因为遭受攻击,或者损坏而无法提供服务的情况下,仍能保持网络连通性的机制。

以太网的容错主要通过生成树协议(Spanning Tree Protocol,STP)实现。生成树协议允许以太网存在冗余链路,但在网络运行时,通过阻塞某些端口使整个网络没有环路,当某条链路因为故障无法通信,或者某台交换机无法工作时,通过重新开通原来阻塞的一些端口,使网络终端之间依然保持连通性,而又没有形成环路,以此实现以太网的容错。

路由器之间由于允许存在环路,因此常通过采用网状拓扑结构来增强 IP 网络的可靠性。

6.2　例题解析

6.2.1　自测题

1. 选择题

(1) 下述________设备不可能具备终端接入控制功能。

A. 交换机　　B. 路由器　　C. AP　　D. 总线

(2) 下述________设备是实施终端接入控制的最佳设备。

A. 交换机　　B. 路由器　　C. 防火墙　　D. 总线

(3) 下述________设备可以用于防止 DHCP 欺骗攻击。

A. 交换机　　B. 路由器　　C. AP　　D. 防火墙

(4) 下述________是路由器实现安全路由的先决条件。

A. 配置相同的共享密钥

B. 路由消息携带消息鉴别码

C. 基于共享密钥和 HMAC 算法产生消息鉴别码

D. 以上全是

(5) 下述________攻击无法窃取传输过程中的数据。

A. DHCP 欺骗攻击　　B. ARP 欺骗攻击

C. 转发表溢出攻击　　D. 源 IP 地址欺骗攻击

(6) 下述________是防止源 IP 地址欺骗攻击的有效手段。

A. 绑定 MAC 地址和 IP 地址　　B. 绑定接入端口和 MAC 地址

C. 绑定接入端口和 IP 地址　　D. 防火墙设置标准过滤器

(7) 下述________是防止 ARP 欺骗攻击的有效手段。

A. 绑定 MAC 地址和 IP 地址　　B. 绑定接入端口和 MAC 地址

C. 绑定接入端口和 IP 地址　　D. 防火墙设置标准过滤器

(8) 访问控制列表是基于________的接入控制技术。

A. 终端 MAC 地址　　B. 授权用户名和口令

C. 终端 IP 地址　　　　　　D. MAC 帧类型

(9) 下述________有关 802.1X 的描述是错误的。

A. 802.1X 是基于用户的接入控制技术

B. 802.1X 和访问控制列表结合才能精细控制终端接入

C. 终端多次接入某个交换机端口只需一次身份鉴别过程

D. 身份鉴别过程中记录授权用户使用的终端的 MAC 地址

(10) 下述________有关安全路由的描述是错误的。

A. RIP 要求交换路由消息的两个相邻路由器配置相同的共享密钥

B. OSPF 要求属于同一区域的路由器接口配置相同的共享密钥

C. OSPF 要求建立邻接关系的两个相邻路由器配置相同的共享密钥

D. 路由消息必须携带共享密钥参与计算的消息鉴别码

(11) 下述________不是划分 VLAN 的原因。

A. 缩小广播域

B. 便于控制 VLAN 间交换的数据

C. 缩小 ARP 欺骗攻击的攻击范围

D. 缩小 DHCP 欺骗攻击的攻击范围

(12) NAT 对防止下述________攻击是无效的。

A. 连接在公共网络上的黑客发起的对内部网络终端的主动攻击

B. 因为下载包含病毒的网页而感染病毒

C. 内部网络终端发起的对外部网络中的服务器的 SYN 泛洪攻击

D. 从外部网络传播蠕虫到内部网络

(13) 下述________有关生成树协议的描述是错误的。

A. 生成树协议允许网状以太网结构

B. 生成树协议允许在存在环路的以太网中传输 MAC 帧

C. 生成树协议通过阻塞一些交换机端口来消除环路且保证连通性

D. 生成树协议自动根据以太网拓扑结构变化调整交换机端口状态

2. 填空题

(1) 以太网安全技术有________、________、________和________，其中________可以防止黑客非法接入网络，________可以缩小 ARP 欺骗攻击的攻击范围，________可以防止源 IP 地址欺骗攻击，________可以防止 DHCP 欺骗攻击。

(2) OSPF 实现安全路由要求做到________、________和________。

(3) 交换机访问控制列表基于________控制终端接入，802.1X 基于________控制终端接入，只有实现________和________的有机结合，才能精确控制授权用户使用的终端接入。

(4) 目前的校园网通常是由多个________互连而成的互连网，它的容错体现在________和________两个方面，其中________容错由生成树协议实现。

(5) NAT 使得内部网络对于外部网络中的终端是________，因此，NAT 能够有效防止外部网络终端对内部网络终端实施________，也可避免________。由于 NAT 需要通

过标准过滤器指定允许地址转换的内部网络私有地址范围，因此内部网络终端访问外部网络资源过程中不容易实现________，因此，也可有效防止内部网络终端对外部网络服务器实施________攻击。

3. 名词解释

____容错	____ VLAN
____ NAT	____安全路由
____ STP	____交换机访问控制列表

(a) 一种通过建立内部网络私有 IP 地址与全球 IP 地址之间映射，使得内部网络分配私有 IP 地址的终端能够访问外部网络资源的技术。

(b) 一种只允许授权路由器之间交换路由消息，对接收到的路由消息进行源端鉴别和完整性检测，并因此使路由表内容和实际网络拓扑结构一致的路由项生成技术。

(c) 一种在网络中的一些物理链路和一些转发结点(如交换机、路由器)因为遭受攻击，或者损坏而无法提供服务的情况下，仍能保持网络连通性的机制。

(d) 一个逻辑以太网，包含的终端可以是某个大型物理以太网终端的任意子集，且子集的分配是动态的，其功能特性等同于包含这些终端的独立物理以太网。

(e) 一种通过在交换机之间交换网桥协议数据单元(Bridge Protocol Data Unit，BPDU)阻塞掉形成环路的交换机端口，从而使网状以太网成为树形以太网的协议。

(f) 一种通过在交换机端口配置 MAC 地址列表，只允许继续转发从该交换机端口输入、且源 MAC 地址属于 MAC 地址列表的 MAC 帧的终端接入控制技术。

4. 判断题

(1) 由直接连接终端的设备实现接入控制是一种理想的情况。

(2) 必须由路由器实现安全路由功能。

(3) 必须由网络设备和网络拓扑结构实现容错。

(4) 有些攻击，如 ARP 欺骗攻击、源 IP 地址欺骗攻击，适合用网络设备提供的安全功能解决。

(5) 仅仅依靠网络设备，就可实现一个既保证连通性，又有一定安全功能的互连网络。

(6) 将不同安全等级的资源配置到不同的 VLAN，从而实施不同的访问控制策略是 VLAN 在网络安全方面的主要应用。

(7) 将默认 VLAN——VLAN 1 和其他 VLAN 隔绝是保证设备管理安全的有效手段。

6.2.2 自测题答案

1. 选择题答案

(1) D，终端接入控制设备必须是智能设备。

(2) A，接入控制最好在直接连接终端的设备上进行。

(3) A，将交换机端口分为信任端口和非信任端口是防止 DHCP 欺骗攻击的有效手段。

(4) D,A、B 和 C 是实现安全路由的三项先决条件。

(5) D,其他三项中 A 和 B 能够改变数据传输路径,C 导致以广播方式传输数据。

(6) C,将 IP 地址和交换机端口绑定,从该交换机端口输入的 IP 分组中,只允许继续传输源 IP 地址为与该交换机端口绑定的 IP 地址的 IP 分组是防止源 IP 地址欺骗攻击的有效手段。

(7) A,ARP 欺骗攻击就是伪造 IP 地址与 MAC 地址的绑定关系。

(8) A,某个交换机端口一旦配置 MAC 地址列表,该交换机端口输入的 MAC 帧中,只允许继续传输源 MAC 地址属于 MAC 地址列表的 MAC 帧。

(9) C,一旦交换机端口检测到该终端离线,或者规定时间内没有接收到该终端发送的 MAC 帧,在重新通过身份鉴别前,该交换机端口将禁止转发该终端发送的 MAC 帧。

(10) C,OSPF 要求某个路由器发送的链路状态更新报文泛洪到整个区域,因此整个区域必须配置相同的共享密钥。

(11) D,DHCP 欺骗攻击的攻击范围不是单个 VLAN。

(12) B,NAT 对内部网络终端访问外部或内部网络中的 Web 服务器没有限制。

(13) B,生成树协议的作用是将网状以太网转变成树形以太网,然后让交换机在树形以太网结构中转发 MAC 帧。

2. 填空题答案

(1) 接入控制,VLAN,IP 地址、MAC 地址和端口三者绑定,信任端口,接入控制,VLAN,IP 地址、MAC 地址和端口三者绑定,信任端口。

(2) 属于相同区域的接口配置相同的共享密钥,路由消息携带消息鉴别码,基于共享密钥和 HMAC 算法产生消息鉴别码。

(3) MAC 地址,用户标识信息,访问控制列表,802.1X。

(4) 以太网,以太网,互连网,以太网。

(5) 透明的,主动攻击,蠕虫病毒从外部网络自动传播到内部网络,源 IP 地址欺骗攻击,SYS 泛洪。

3. 名词解释答案

c 容错	d VLAN
a NAT	b 安全路由
e STP	f 交换机访问控制列表

4. 判断题答案

(1) 对,可以将非法终端隔离在网络外边。

(2) 对,必须由路由器通过和其他路由器交换路由消息建立路由表。

(3) 对,容错就是保证在某些物理链路或网络设备丧失功能的情况下,仍能保持网络的连通性,这只能通过精心设计网络拓扑结构和配置冗余的网络设备实现。

(4) 对,防止这些攻击需要绑定 IP 地址、MAC 地址和交换机端口,通常在直接连接终端的交换机中配置这三者的绑定关系。

(5) 对,网络设备本身具有许多安全功能。

(6) 对,防火墙访问控制策略主要用于控制网络间的信息交换过程,VLAN 等同于一

个独立的以太网。

（7）对，这样可以保证只允许连接在VLAN 1中的终端对设备实施远程配置。

6.2.3　简答题解析

1. 简述网络设备提供的安全功能的重要性。

回答：一是最好由直接连接终端的设备，如交换机实现接入控制，这样才能完全将非法终端隔离在网络外面。二是有些攻击行为只能依靠网络设备予以防止，如防止DHCP欺骗攻击需要网络设备禁止伪造的DHCP服务器向网络发送DHCP响应报文。三是信息截获攻击通常需要改变数据传输路径，网络设备的安全功能能够确保建立并维持的端到端传输路径是正确的。四是容错网络结构能够增强网络的可用性，而网络的可用性是保证信息可用性的基础。五是一切数据必须经过网络设备才能实现传输过程。因此，网络设备是对经过网络传输的数据实施检测、监控的理想之处。

2. 简述NAT的安全功能。

回答：一是由于分配私有IP地址的内部网络对于外部网络是透明的，因此连接在外部网络上的黑客终端无法对内部网络终端发起主动攻击。二是在建立内部网络私有IP地址和全球IP地址之间映射前，外部网络终端无法主动和内部网络终端通信，因此蠕虫病毒很难自动地从外部网络传播到内部网络。三是由于需要通过标准过滤器指定允许进行地址转换的内部网络私有IP地址范围，因此内部网络终端无法通过伪造的不存在的内部网络地址去访问外部网络服务器，从而无法对外部网络服务器实施SYN泛洪攻击。

3. 简述Internet接入控制和802.1X接入控制的不同。

回答：Internet接入控制和802.1X接入控制都需完成用户身份鉴别，需要通过身份鉴别确定用户是授权用户。但Internet接入控制设备在完成用户身份鉴别后，将分配给该用户终端的IP地址和连接该用户终端的点对点信道，或者PPP会话作为该用户的标识符，接入控制设备确定某个IP分组是否是该授权用户发送的IP分组的依据是：①IP分组的源IP地址是否是分配给该用户的IP地址，②该IP分组是否从连接该用户终端的对点对信道，或PPP会话到达。Internet接入控制设备必须是实现接入网络与Internet互连，且能够在接入网络和Internet之间完成IP分组转发的路由设备。

802.1X接入控制设备在完成用户身份鉴别后，将该用户终端的MAC地址作为该用户的标识符，接入控制设备确定某个MAC帧是否是该授权用户发送的MAC帧的依据是：该MAC帧的源MAC地址是否是完成身份鉴别时接入控制设备记录下的用户终端的MAC地址。802.1X接入控制设备必须是MAC帧转发设备，交换机和具有以太网接口的路由器均可是802.1X接入控制设备。

6.3　实　　验

6.3.1　安全校园网设计实验

1. 实验内容

（1）完成VLAN划分和配置。

(2) 完成交换机接入控制配置。

(3) 完成三层交换机 IP 接口配置

(4) 完成安全路由配置。

(5) 实现访问控制策略。

2. 网络结构

校园网结构如图 6.1 所示。将整个网络划分为 7 个 VLAN,其中三层交换机 S5 中定义 VLAN 2 和 VLAN 5 对应的 IP 接口,VLAN 5 为互连三层交换机 S5 和 S7 的网络。三层交换机 S6 中定义 VLAN 4 和 VLAN 6 对应的 IP 接口,VLAN 6 为互连三层交换机 S6 和 S7 的网络。三层交换机 S7 中定义 VLAN 3、VLAN 7、VLAN 8、VLAN 5 和 VLAN 6 对应的 IP 接口。图 6.2 是图 6.1 所示物理结构按照上述 IP 接口定义后形成的逻辑结构。

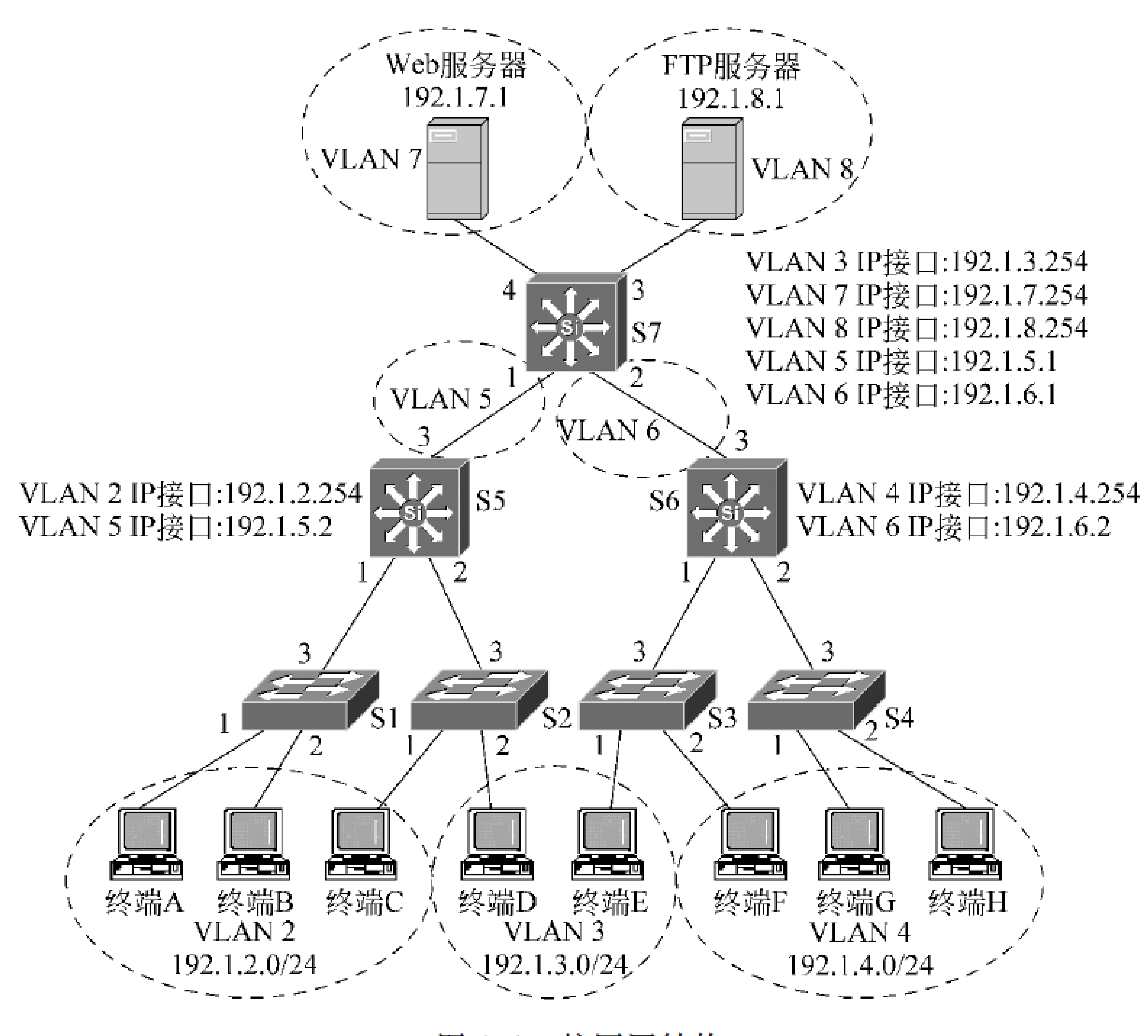


图 6.1 校园网结构

交换机 VLAN 配置必须保证:一是属于同一 VLAN 的两个终端之间必须存在交换路径,二是属于某个 VLAN 的终端必须存在该终端与该 VLAN 对应的 IP 接口之间的交换路径。对于每一个交换机端口,如果该交换机端口只有单条属于某个 VLAN 的交换路径经过,该交换机端口作为非标记端口分配给该 VLAN;如果该交换机端口被多条属于不同 VLAN 的交换路径经过,该交换机端口作为标记端口被这些 VLAN 共享。根据上述配置原则,得出表 6.1 所示的交换机端口 VLAN 配置。

S5、S6 和 S7 构成 OSPF 一个区域,为了实现安全路由,路由器必须对接收到的路由消息进行源端鉴别和完整性检测。因此,相同区域内的每一个路由器必须配置相同的

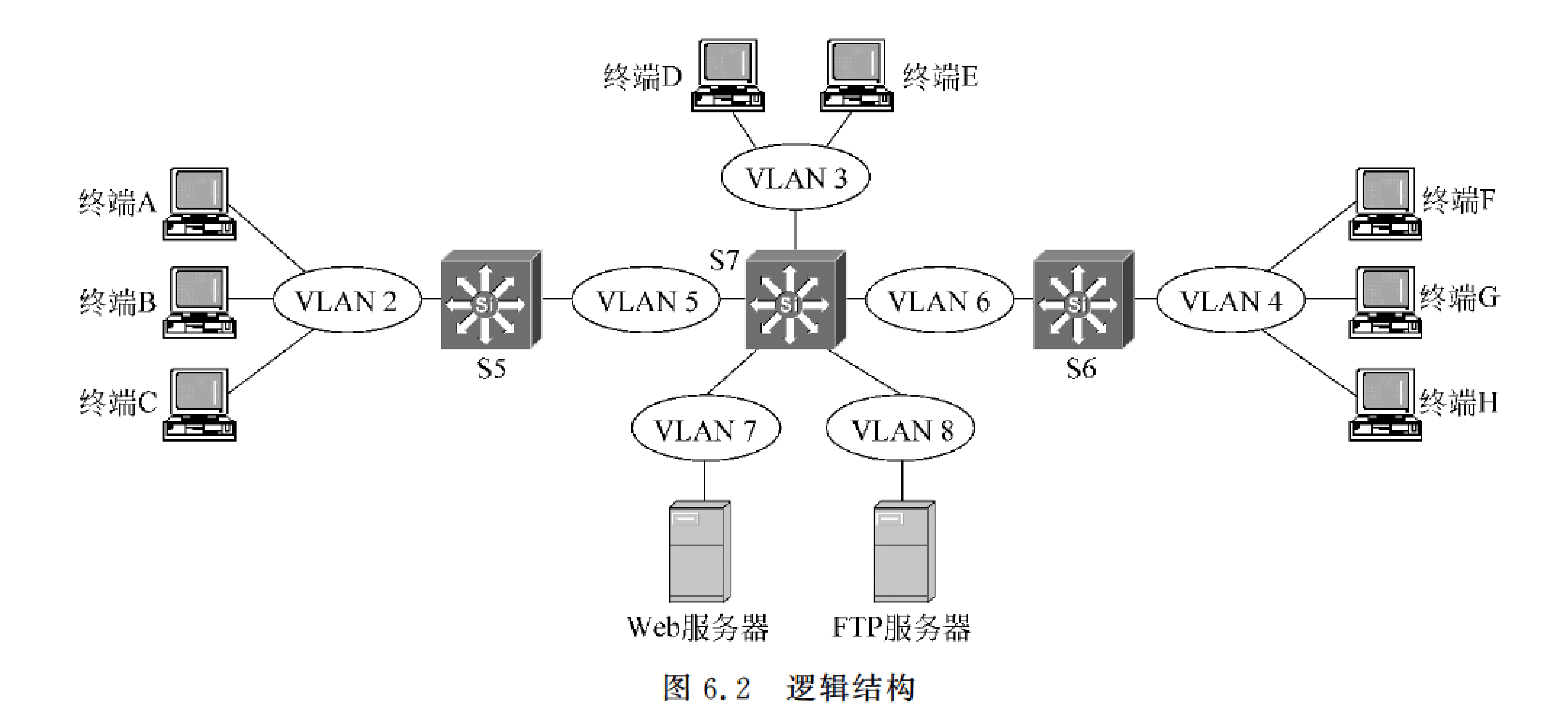


图 6.2　逻辑结构

表 6.1　交换机端口 VLAN 配置

VLAN	非标记端口	标记端口
VLAN 2	S1.1、S1.2、S1.3、S5.1、S2.1	S2.3、S5.2
VLAN 3	S2.2、S3.1	S2.3、S5.2、S5.3、S3.3、S6.1、S6.3、S7.1、S7.2
VLAN 4	S3.2、S4.1、S4.2、S4.3、S6.2	S3.3、S6.1
VLAN 5		S5.3、S7.1
VLAN 6		S6.3、S7.2
VLAN 7	S7.4	
VLAN 8	S7.3	

注：S1.1 表示 S1 交换机的端口 1。

共享密钥，在发送的 OSPF 报文中附加由 HAMC-MD5-128 算法生成的消息鉴别码(MAC)。

接入交换机(S1～S4)的每一个端口通过配置访问控制列表只允许接入 MAC 地址为指定地址的终端。

为了防止终端实施源 IP 地址欺骗攻击，通过在 VLAN 2、VLAN 3 和 VLAN 4 对应的 IP 接口输入方向上设置标准过滤器，只允许源 IP 地址和分配给该 VLAN 的网络地址一致的 IP 分组继续转发。

通过配置访问控制策略，只允许 VLAN 2 内的终端访问 Web 服务器和 FTP 服务器，只允许 VLAN 3 内的终端访问 Web 服务器，不允许其他 VLAN 内的终端访问任何服务器。

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 6.1 所示的网络结构放置和连接设备，逻辑工作区完成设备放置和连接后的界面如图 6.3 所示。

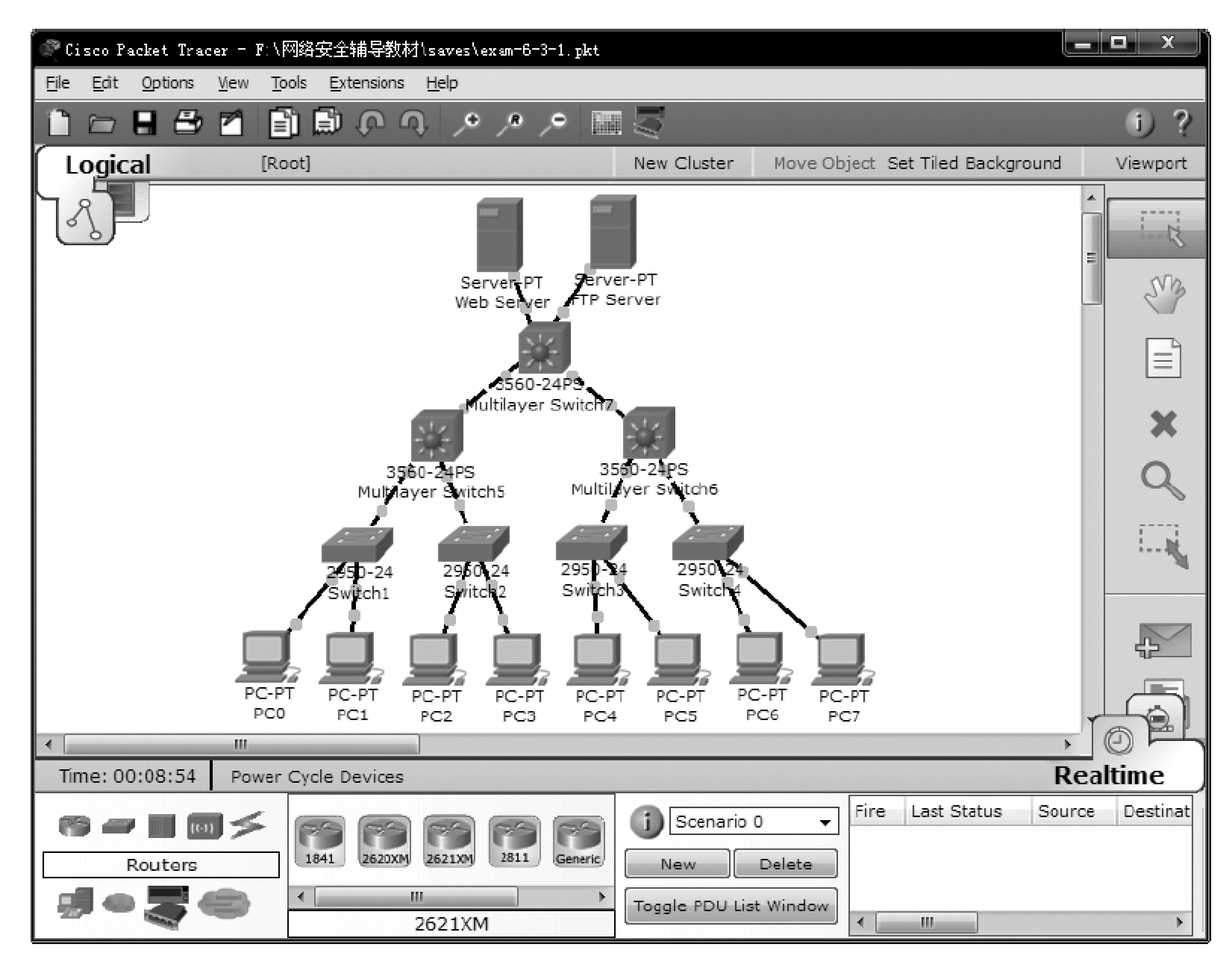


图 6.3 放置和连接设备后的逻辑工作区界面

(2) 在各个交换机(包括二层和三层交换机)中创建 VLAN,为每一个 VLAN 分配交换机端口。图 6.4 是在 Switch2 中创建 VLAN 的界面,图 6.5 是将端口分配给 VLAN 的界面。如果某个三层交换机端口被配置成被多个 VLAN 共享的标记端口(Trunk 端口),需要通过命令"switchport trunk encapsulation dot1q"将进出该端口的 MAC 帧的封装格式定义为 802.1Q 格式。

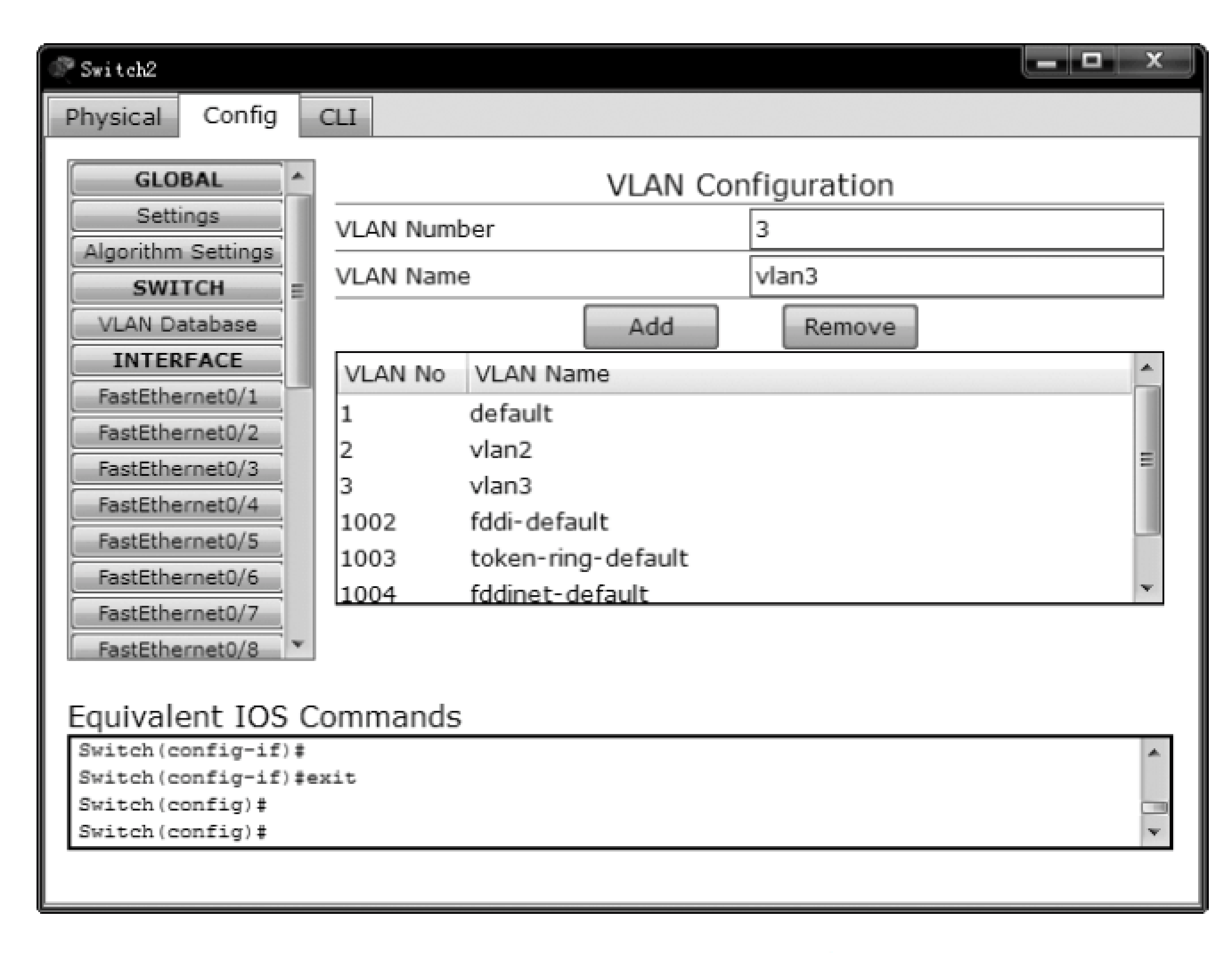


图 6.4 Switch2 配置 VLAN 的界面

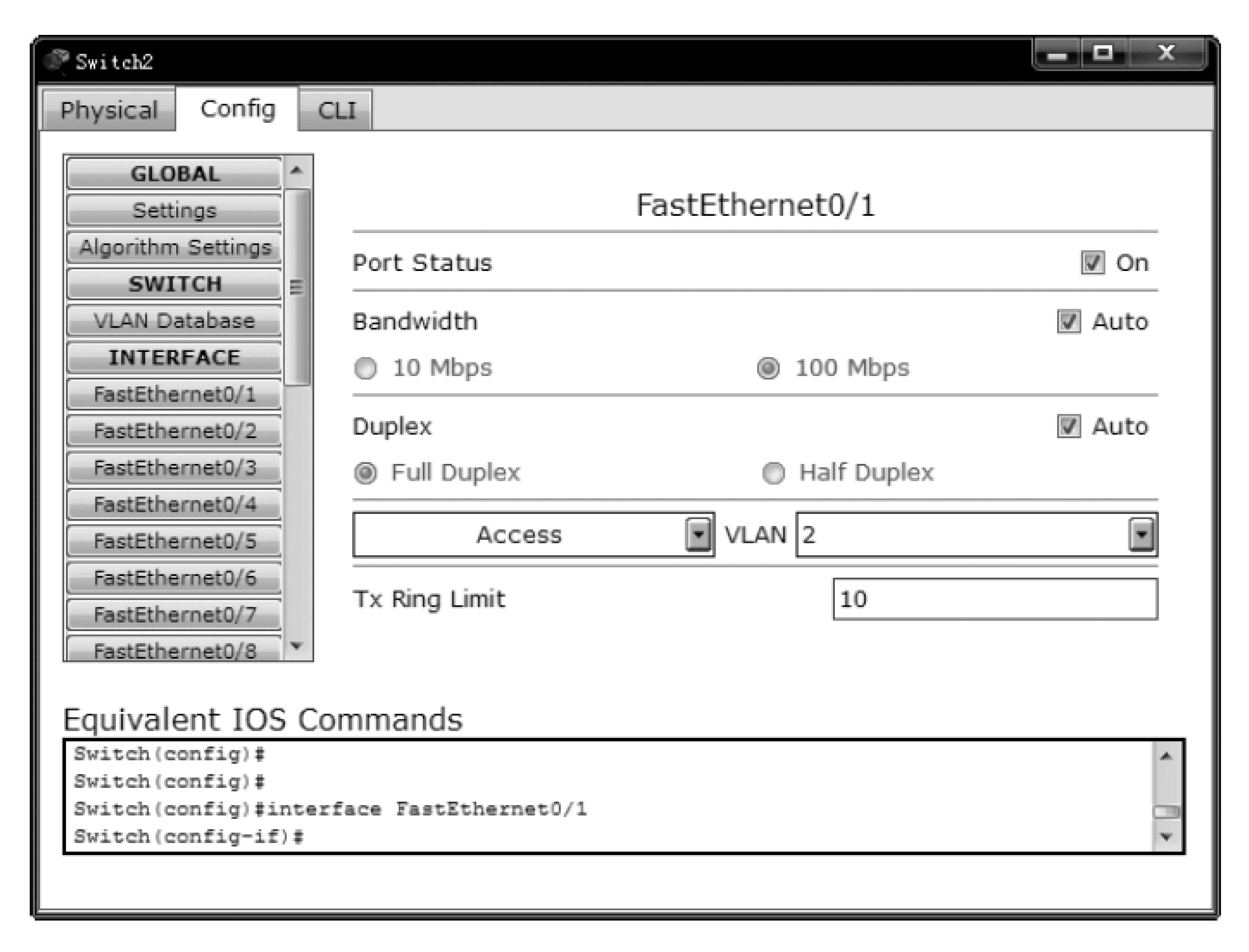


图 6.5　Switch2 端口配置界面

(3) 在每一个连接终端的二层交换机端口中配置访问控制列表，只允许 MAC 地址为访问控制列表中指定地址的终端接入该交换机端口，并通过该交换机端口发送、接收 MAC 帧。

(4) 在三层交换机中定义 IP 接口，分配 IP 地址和子网掩码。如果在 Switch5 中定义了 VLAN 2 和 VLAN 5 对应的 IP 接口，在 Switch6 中定义了 VLAN 4 和 VLAN 6 对应的 IP 接口，Switch7 中定义了 VLAN 3、VLAN 5、VLAN 6、VLAN 7 和 VLAN 8 对应的 IP 接口，并为每一个 IP 接口分配了 IP 地址和子网掩码，三个三层交换机中产生图 6.6～图 6.8 所示的路由表。IP 接口和子网掩码确定了对应 VLAN 的网络地址，连接在该 VLAN 中的终端分配的 IP 地址必须与该网络地址一致，并以 IP 接口的 IP 地址作为默认网关地址。如果 Switch5 中为 VLAN 2 对应的 IP 接口分配 IP 地址和子网掩码 192.1.2.254/24，VLAN 2 的网络地址是 192.1.2.0/24，PC0 分配的 IP 地址、子网掩码和默认网关地址如图 6.9 所示。

Routing Table for Multilayer Switch5

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	Vlan2	---	0/0
C	192.1.5.0/24	Vlan5	---	0/0

图 6.6　Switch5 完成 IP 接口配置后的初始路由表

Routing Table for Multilayer Switch6

Type	Network	Port	Next Hop IP	Metric
C	192.1.4.0/24	Vlan4	---	0/0
C	192.1.6.0/24	Vlan6	---	0/0

图 6.7　Switch6 完成 IP 接口配置后的初始路由表

Routing Table for Multilayer Switch7

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	Vlan3	---	0/0
C	192.1.5.0/24	Vlan5	---	0/0
C	192.1.6.0/24	Vlan6	---	0/0
C	192.1.7.0/24	Vlan7	---	0/0
C	192.1.8.0/24	Vlan8	---	0/0

图 6.8 Switch7 完成 IP 接口配置后的初始路由表

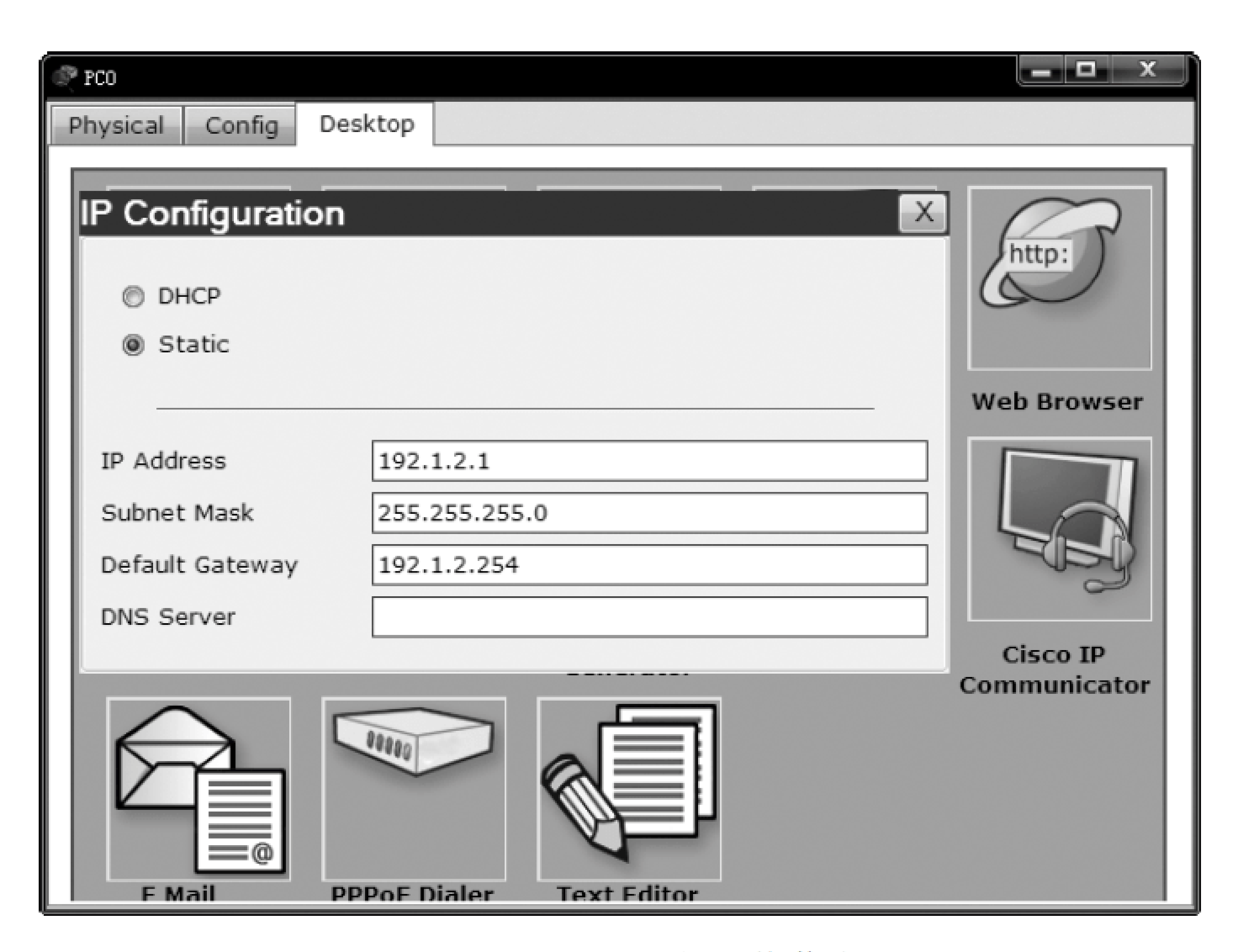


图 6.9 PC0 配置的网络信息

（5）将三层交换机 Switch5、Switch6 和 Switch7 定义为一个区域——区域 1，在每一个三层交换机中配置参与区域 1 OSPF 动态路由项建立的网络和接口，配置区域 1 的鉴别算法和共享密钥。在参与区域 1 OSPF 动态路由项建立的所有接口中配置鉴别算法和共享密钥。需要指出的是，不同三层交换机参与同一区域 OSPF 动态路由项建立的所有接口需配置相同的鉴别算法和共享密钥。三层交换机 Switch5、Switch6 和 Switch7 包含 OSPF 动态路由项的完整路由表如图 6.10～图 6.12 所示。此时，已经实现校园网终端之间、终端与服务器之间的连通性。可以通过 Ping 操作验证校园网终端之间、终端与服务器之间的连通性。

Routing Table for Multilayer Switch5

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	Vlan2	---	0/0
C	192.1.5.0/24	Vlan5	---	0/0
O	192.1.3.0/24	Vlan5	192.1.5.1	110/2
O	192.1.4.0/24	Vlan5	192.1.5.1	110/3
O	192.1.6.0/24	Vlan5	192.1.5.1	110/2
O	192.1.7.0/24	Vlan5	192.1.5.1	110/2
O	192.1.8.0/24	Vlan5	192.1.5.1	110/2

图 6.10 Switch5 完整路由表

(6) 为了防止连接在 VLAN 2、VLAN 3 和 VLAN 4 上的终端实施源 IP 地址欺骗攻击，在 VLAN 2、VLAN 3 和 VLAN 4 对应的 IP 接口输入方向上设置标准过滤器，过滤掉一切源 IP 地址与 VLAN 网络地址不一致的 IP 分组。PC0 连接在 VLAN 2 上，PC0 的 IP 地址必须属于网络地址 192.1.2.0/24，如果 PC0 发送图 6.13 所示的源 IP 地址伪装为 192.1.3.2 的 IP 分组，由于该 IP 分组的源 IP 地址和 VLAN 2 的网络地址不一致，VLAN 2 对应的 IP 接口将隔断该 IP 分组，如图 6.14 所示。

Routing Table for Multilayer Switch6

Type	Network	Port	Next Hop IP	Metric
C	192.1.4.0/24	Vlan4	---	0/0
C	192.1.6.0/24	Vlan6	---	0/0
O	192.1.2.0/24	Vlan6	192.1.6.1	110/3
O	192.1.3.0/24	Vlan6	192.1.6.1	110/2
O	192.1.5.0/24	Vlan6	192.1.6.1	110/2
O	192.1.7.0/24	Vlan6	192.1.6.1	110/2
O	192.1.8.0/24	Vlan6	192.1.6.1	110/2

图 6.11　Switch6 完整路由表

Routing Table for Multilayer Switch7

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	Vlan3	---	0/0
C	192.1.5.0/24	Vlan5	---	0/0
C	192.1.6.0/24	Vlan6	---	0/0
C	192.1.7.0/24	Vlan7	---	0/0
C	192.1.8.0/24	Vlan8	---	0/0
O	192.1.2.0/24	Vlan5	192.1.5.2	110/2
O	192.1.4.0/24	Vlan6	192.1.6.2	110/2

图 6.12　Switch7 完整路由表

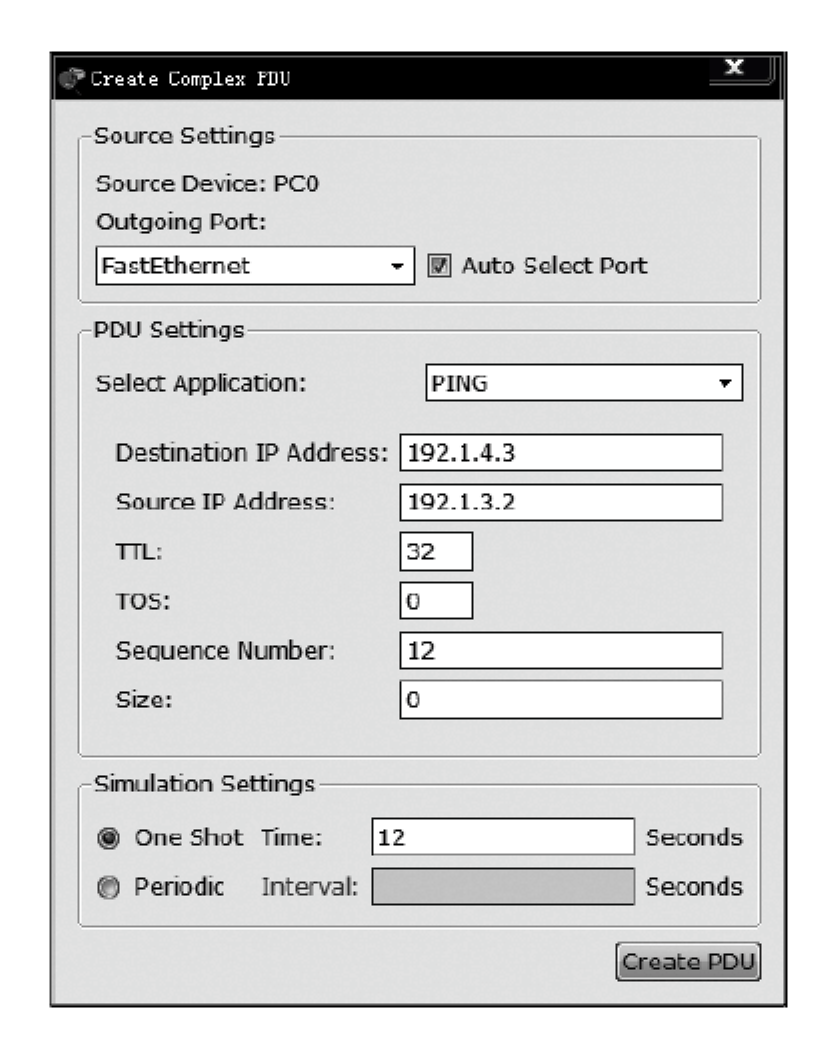


图 6.13　PC0 创建的用于源 IP 地址欺骗攻击的 ICMP 报文

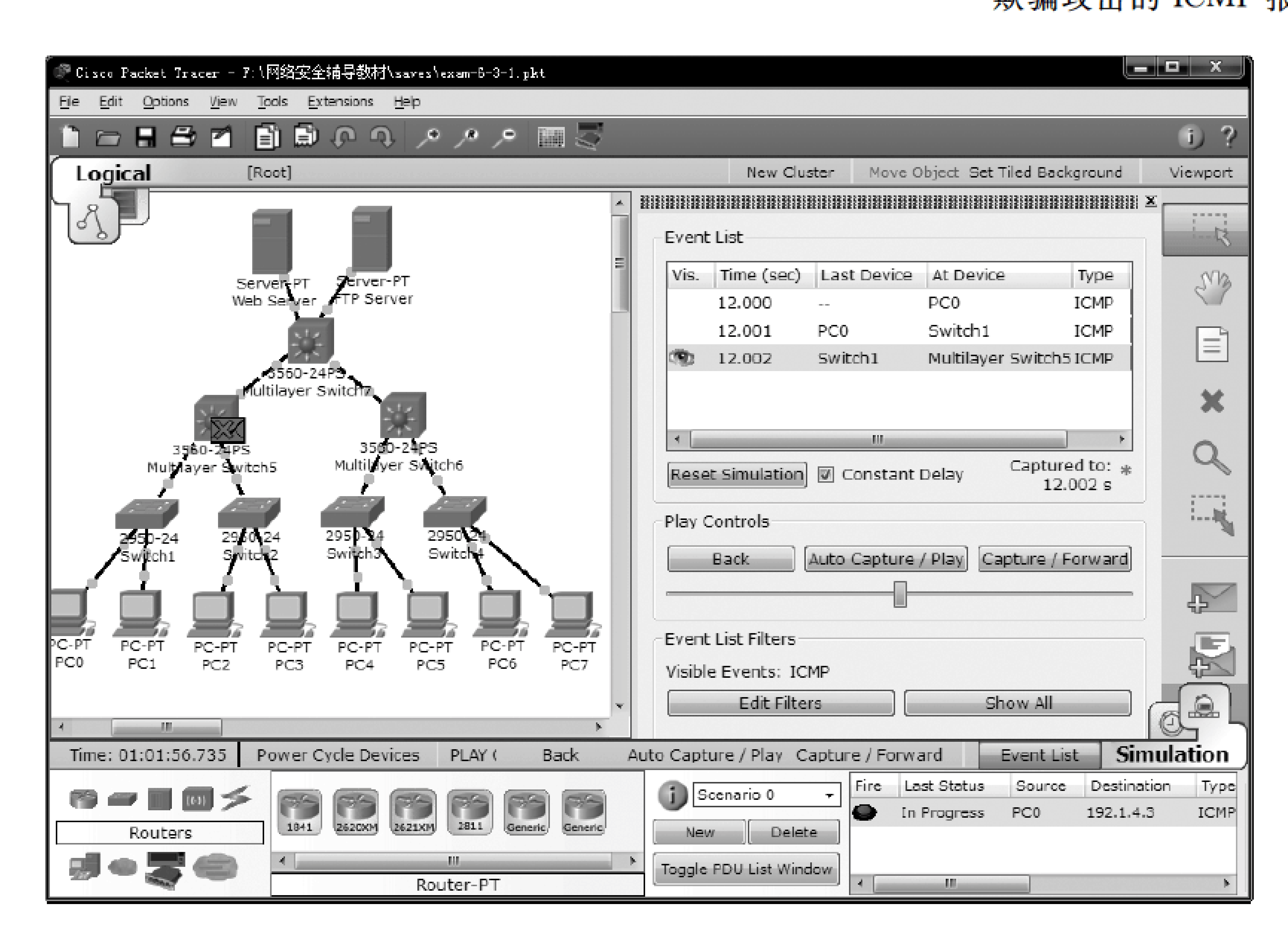


图 6.14　PC0 源 IP 地址欺骗攻击报文被阻隔

(7) 在 VLAN 7 对应的 IP 接口的输出方向设置只允许源 IP 地址属于网络 192.1.2.0/24 和网络 192.1.3.0/24,目的 IP 地址为 Web 服务器 IP 地址 192.1.7.1/32,目的端口号为 HTTP 对应的著名端口号的 TCP 报文进入 VLAN 7 的扩展分组过滤器。在 VLAN 8 对应的 IP 接口的输出方向设置只允许源 IP 地址属于网络 192.1.2.0/24,目的 IP 地址为 FTP 服务器 IP 地址 192.1.8.1/32,目的端口号为 FTP 对应的著名端口号的 TCP 报文进入 VLAN 8 的扩展分组过滤器。连接在 VLAN 3 上的终端允许访问 Web 服务器。图 6.15 是 PC4 成功访问 Web 服务器的界面,但不允许访问 FTP 服务器。图 6.16 是 PC4 访问 FTP 服务器失败的界面。连接在 VLAN 2 上的终端允许访问 Web 服务器和 FTP 服务器。图 6.17 是 PC0 成功访问 FTP 服务器的界面。连接在 VLAN 4 上的终端不允许访问 Web 服务器和 FTP 服务器。图 6.18 是 PC7 访问 Web 服务器失败的界面。

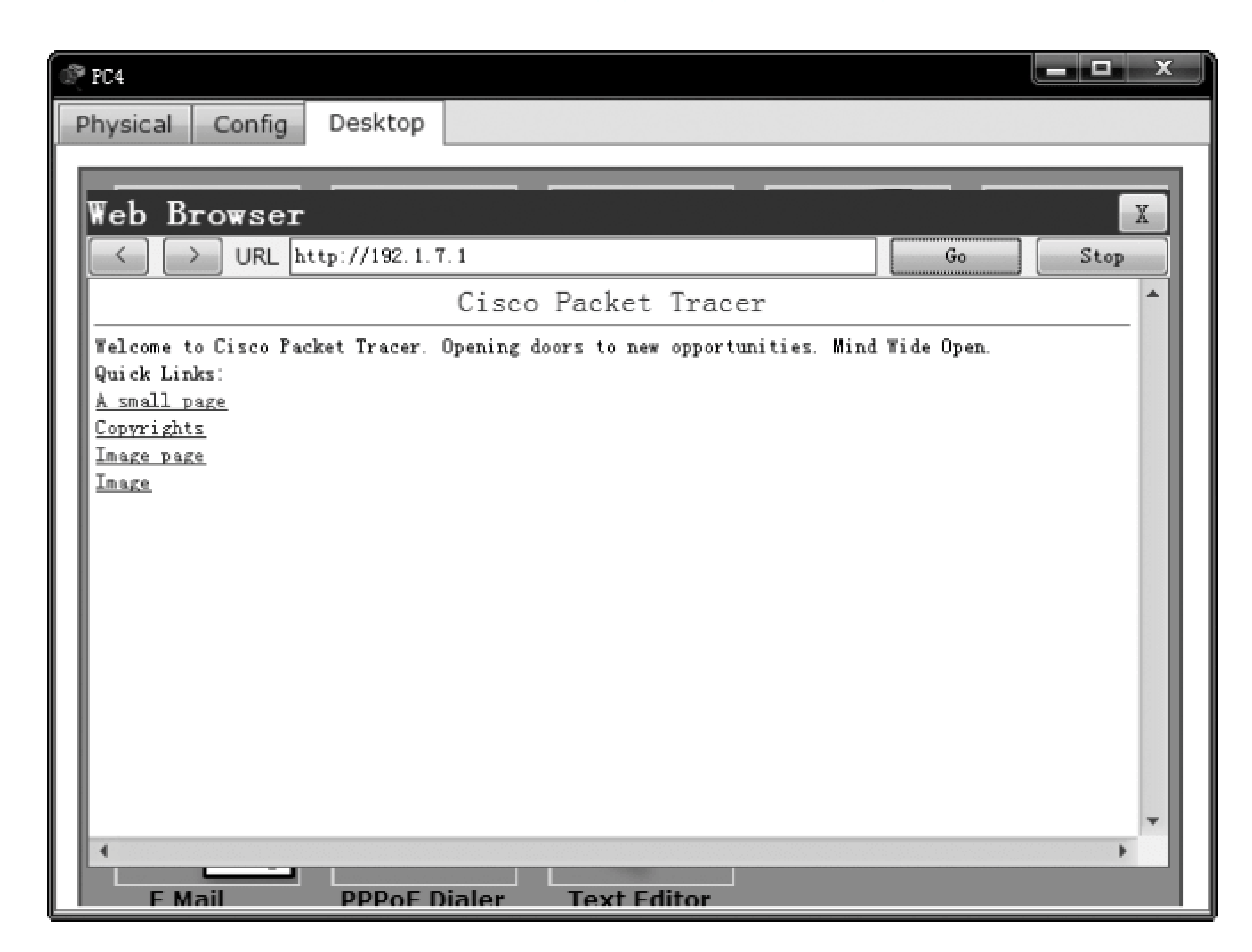


图 6.15 PC4 成功访问 Web 服务器的界面

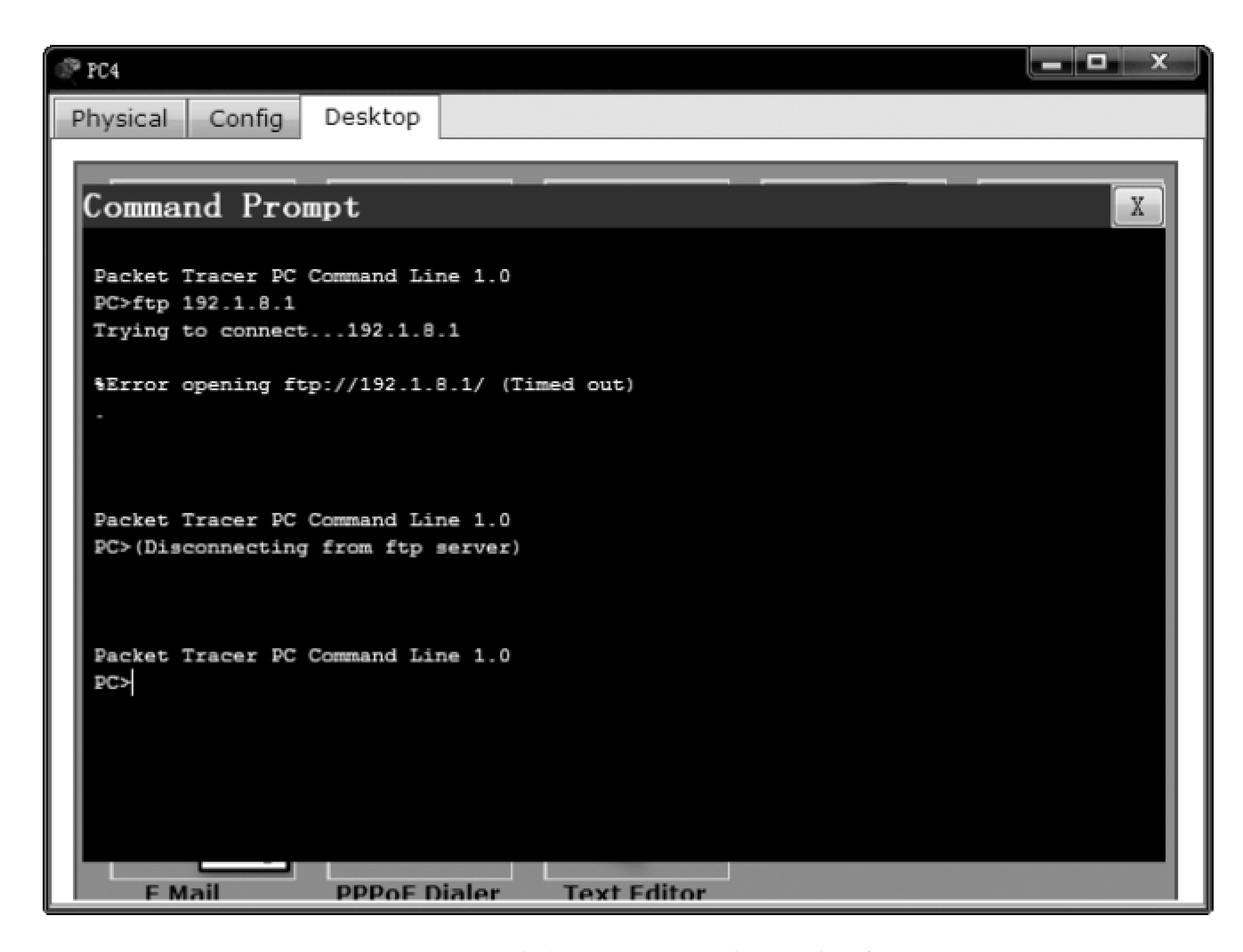


图 6.16 PC4 访问 FTP 服务器失败的界面

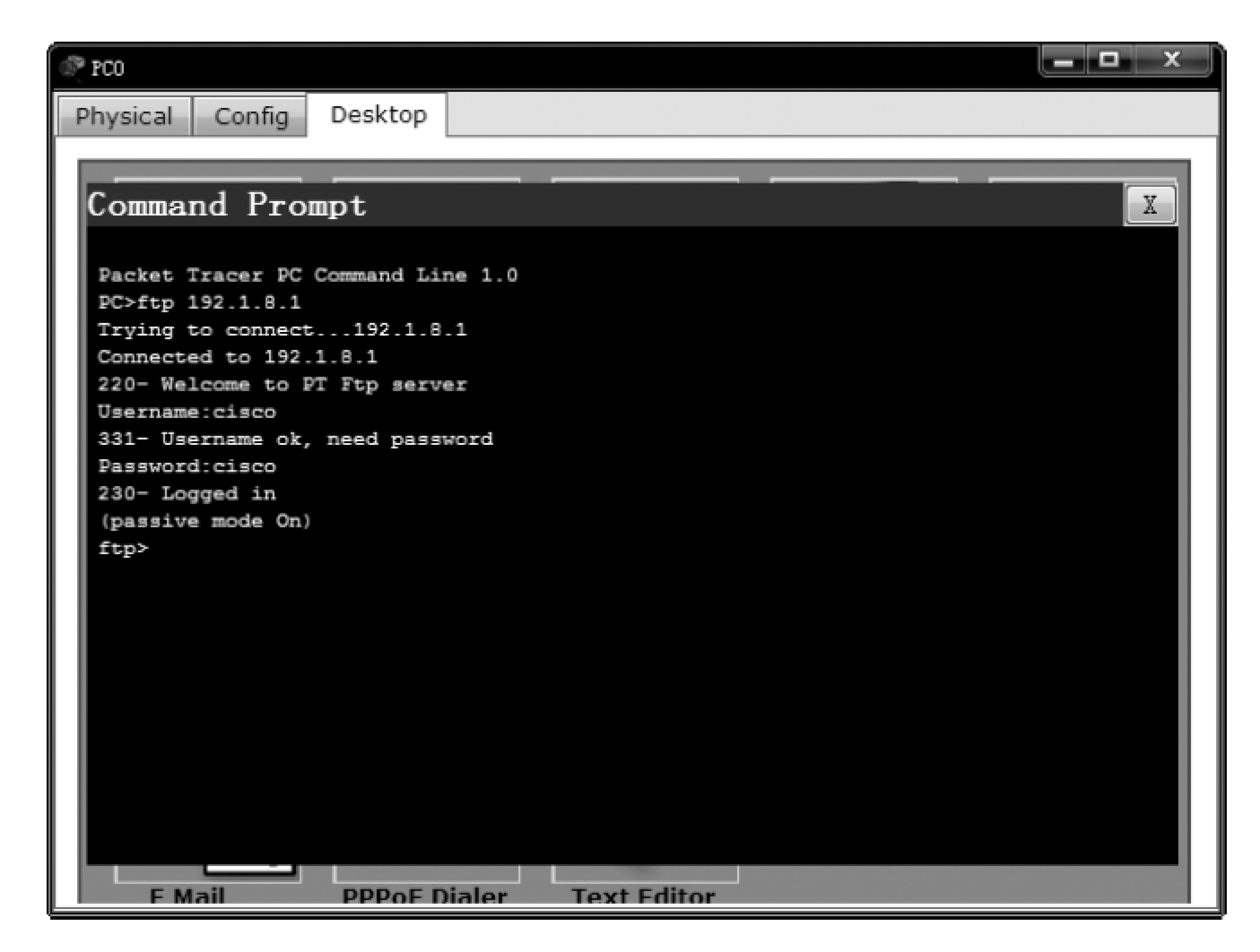


图 6.17　PC0 成功访问 FTP 服务器的界面



图 6.18　PC7 访问 Web 服务器失败的界面

4. 命令行配置过程

(1) Switch2 命令行配置过程。

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 2                    (创建编号为 2 的 VLAN)
Switch(config-vlan)#name vlan2           (为该 VLAN 取名为 vlan2)
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
```

```
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 2
                        (将端口作为非标记端口分配给编号为 2 的 VLAN)
Switch(config-if)#switchport mode access
                        (指定端口模式为静态非标记端口,静态模式是启动端口安全功能的前提)
Switch(config-if)#switchport port-security      (启动端口安全功能)
Switch(config-if)#switchport port-security maximum 1
                        (将访问控制列表中 MAC 地址数上限设置为 1)
Switch(config-if)#switchport port-security mac-address 0001.9763.B6E8
                        (将 MAC 地址 0001.9763.B6E8 静态配置到访问控制列表中)
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 3
Switch(config-if)#switchport mode access
Switch(config-if)#exit Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0001.9759.20EC
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode trunk      (指定端口模式为静态标记端口)
Switch(config-if)#switchport trunk allowed vlan 2,3
                                            (VLAN 2 和 VLAN 3 共享该标记端口)
Switch(config-if)#exit
```

其他二层交换机命令行配置过程与此相似,不再赘述。

(2) Switch5 命令行配置过程。

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 2
Switch(config-vlan)#name vlan2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
Switch(config-vlan)#exit
Switch(config)#vlan 5
Switch(config-vlan)#name vlan5
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport trunk encapsulation dot1q
                                          (指定 802.1Q 为端口作为标记端口时的封装格式)
Switch(config-if)#switchport mode trunk      (指定端口模式为静态标记端口)
```

```
Switch(config-if)#switchport trunk allowed vlan 2,3      (VLAN 2和VLAN 3共享该标记端口)
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 3,5
Switch(config-if)#exit
Switch(config)#interface vlan 2                (定义编号为2的VLAN对应的IP接口)
Switch(config-if)#ip address 192.1.2.254 255.255.255.0
                                   (为该IP接口分配IP地址和子网掩码192.1.2.254/24)
Switch(config-if)#exit
Switch(config)#interface vlan 5
Switch(config-if)#ip address 192.1.5.2 255.255.255.0
Switch(config-if)#exit
Switch(config)#router ospf 5                   (启动进程标识符为5的OSPF进程,
Switch(config-router)#network 192.1.2.0 0.0.0.255 area 1
        (定义参与区域1动态路由项建立过程的网络和接口,网络192.1.2.0/24及IP地址属于
         该网络的接口参与区域1动态路由项建立过程)
Switch(config-router)#network 192.1.5.0 0.0.0.255 area 1
Switch(config-router)#area 1 authentication message-digest
              (要求对区域1中传播的OSPF报文进行源端鉴别和完整性检测,并指定鉴别算法)
Switch(config-router)#exit
Switch(config)#interface vlan 2      (进入参与区域1中OSPF动态路由项建立过程的IP接口)
Switch(config-if)#ip ospf authentication message-digest
                                   (要求对发送的OSPF报文附加消息鉴别码,同时对
                                    接收到的OSPF报文进行源端鉴别和完整性检测)
Switch(config-if)#ip ospf message-digest-key 1 md5 1234
                                   (指定消息鉴别码生成算法及密钥)
Switch(config-if)#exit
Switch(config)#interface vlan 5
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#ip ospf message-digest-key 1 md5 1234
Switch(config-if)#exit
Switch(config)#access-list 1 permit 192.1.2.0 0.0.0.255
             (配置只允许继续转发源IP地址属于网络地址192.1.2.0/24的IP分组的过滤规则)
Switch(config)#access-list 1 deny any           (配置拒绝一切IP分组的过滤规则)
Switch(config)#interface vlan 2
Switch(config-if)#ip access-group 1 in
     (将该标准过滤器作用到IP接口输入方向,实际上只允许源IP地址属于分配给VLAN 2的网络
      地址的IP分组离开VLAN 2,防止连接在VLAN 2中的终端实施源IP地址欺骗攻击)
Switch(config-if)#exit
```

(3) Switch6命令行配置过程。

```
Switch>enable
```

```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# name vlan3
Switch(config-vlan)# exit
Switch(config)# vlan 4
Switch(config-vlan)# name vlan4
Switch(config-vlan)# exit
Switch(config)# vlan 6
Switch(config-vlan)# name vlan6
Switch(config-vlan)# exit
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 3,4
Switch(config-if)# exit
Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport access vlan 4
Switch(config-if)# exit
Switch(config)# interface FastEthernet0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 3,6
Switch(config-if)# exit
Switch(config)# interface vlan 4
Switch(config-if)# ip address 192.1.4.254 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan 6
Switch(config-if)# ip address 192.1.6.2 255.255.255.0
Switch(config-if)# exit
Switch(config)# router ospf 6
Switch(config-router)# network 192.1.4.0 0.0.0.255 area 1
Switch(config-router)# network 192.1.6.0 0.0.0.255 area 1
Switch(config-router)# area 1 authentication message-digest
Switch(config-router)# exit
Switch(config)# interface vlan 4
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)# ip ospf message-digest-key 1 md5 1234
        (所有参与区域 1 中 OSPF 动态路由项建立过程的 IP 接口需配置相同的鉴别算法和密钥)
Switch(config-if)# exit
Switch(config)# interface vlan 6
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)# ip ospf message-digest-key 1 md5 1234
Switch(config-if)# exit
Switch(config)# access-list 1 permit 192.1.4.0 0.0.0.255
```

```
Switch(config)#access-list 1 deny any
Switch(config)#interface vlan 4
Switch(config-if)#ip access-group 1 in
Switch(config-if)#exit
```

(4) Switch7 命令行配置过程。

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
Switch(config-vlan)#exit
Switch(config)#vlan 5
Switch(config-vlan)#name vlan5
Switch(config-vlan)#exit
Switch(config)#vlan 6
Switch(config-vlan)#name vlan6
Switch(config-vlan)#exit
Switch(config)#vlan 7
Switch(config-vlan)#name vlan7
Switch(config-vlan)#exit
Switch(config)#vlan 8
Switch(config-vlan)#name vlan8
Switch(config-vlan)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 3,5
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 3,6
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 8
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#switchport access vlan 7
Switch(config-if)#exit
Switch(config)#interface vlan 3
Switch(config-if)#ip address 192.1.3.254 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 5
Switch(config-if)#ip address 192.1.5.1 255.255.255.0
```

```
Switch(config-if)#exit
Switch(config)#interface vlan 6
Switch(config-if)#ip address 192.1.6.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 7
Switch(config-if)#ip address 192.1.7.254 255.255.255.0
Switch(config-if)#exit
Switch(config)#interface vlan 8
Switch(config-if)#ip address 192.1.8.254 255.255.255.0
Switch(config-if)#exit
Switch(config)#router ospf 7
Switch(config-router)#network 192.1.3.0 0.0.0.255 area 1
Switch(config-router)#network 192.1.5.0 0.0.0.255 area 1
Switch(config-router)#network 192.1.6.0 0.0.0.255 area 1
Switch(config-router)#network 192.1.7.0 0.0.0.255 area 1
Switch(config-router)#network 192.1.8.0 0.0.0.255 area 1
Switch(config-router)#area 1 authentication message-digest
Switch(config-router)#exit
Switch(config)#interface vlan 3
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#ip ospf message-digest-key 1 md5 1234
            (所有参与区域 1 中 OSPF 动态路由项建立过程的 IP 接口需配置相同的鉴别算法和密钥)
Switch(config-if)#exit
Switch(config)#interface vlan 5
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#ip ospf message-digest-key 1 md5 1234
Switch(config-if)#exit
Switch(config)#interface vlan 6
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#ip ospf message-digest-key 1 md5 1234
Switch(config-if)#exit
Switch(config)#interface vlan 7
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#ip ospf message-digest-key 1 md5 1234
Switch(config-if)#exit
Switch(config)#interface vlan 8
Switch(config-if)#ip ospf authentication message-digest
Switch(config-if)#ip ospf message-digest-key 1 md5 1234
Switch(config-if)#exit
Switch(config)#access-list 1 permit 192.1.3.0 0.0.0.255
Switch(config)#access-list 1 deny any
Switch(config)#interface vlan 3
Switch(config-if)#ip access-group 1 in
Switch(config-if)#exit
```

```
Switch(config)#access-list 101 permit tcp 192.1.2.0 0.0.0.255 host 192.1.7.1 eq www
        (配置允许继续转发源 IP 地址属于网络 192.1.2.0/24、目的 IP 地址为 192.1.7.1/32、目的
        端口号为 HTTP 对应的著名端口号的 TCP 报文的过滤规则)
Switch(config)#access-list 101 permit tcp 192.1.3.0 0.0.0.255 host 192.1.7.1 eq www
        (配置允许继续转发源 IP 地址属于网络 192.1.3.0/24、目的 IP 地址为 192.1.7.1/32、目的
        端口号为 HTTP 对应的著名端口号的 TCP 报文的过滤规则)
Switch(config)#access-list 101 deny ip any any    (配置拒绝一切 IP 分组的过滤规则)
Switch(config)#access-list 102 permit tcp 192.1.2.0 0.0.0.255 host 192.1.8.1 eq ftp
        (配置允许继续转发源 IP 地址属于网络 192.1.2.0/24、目的 IP 地址为 192.1.8.1/32、目的
        端口号为 FTP 对应的著名端口号的 TCP 报文的过滤规则)
Switch(config)#access-list 102 deny ip any any
Switch(config)#interface vlan 7
Switch(config-if)#ip access-group 101 out
        (将编号为 101 的扩展过滤器作用于 VLAN 7 对应的 IP 接口的输出方向,表明只允许连接
        在 VLAN 2 和 VLAN 3 上的终端访问 Web 服务器)
Switch(config-if)#exit
Switch(config)#interface vlan 8
Switch(config-if)#ip access-group 102 out
        (将编号为 102 的扩展过滤器作用于 VLAN 8 对应的 IP 接口的输出方向,表明只允许连接
        在 VLAN 2 上的终端访问 FTP 服务器)
Switch(config-if)#exit
```

6.3.2　容错网络设计实验

1. 实验内容

(1) 配置生成树协议。

(2) 配置容错网络。

(3) 验证容错网络的容错功能。

2. 网络结构

容错网络结构如图 6.19 所示。二层交换机 S1～S4 构成一个容错以太网,容错网络在某些互连交换机的链路损坏,甚至交换机损坏的情况下,仍能保持终端 A 和终端 B 之间的连通性。二层交换机 S5～S8 同样构成一个容错以太网。

每一个终端存在两个第一跳路由器,如果路由器支持热备份路由器协议(Hot Standby Router Protocol,HSRP),终端配置的默认网关地址可以是一个虚拟 IP 地址,HSRP 能够自动将该虚拟 IP 地址映射到其中一个路由器接口的 IP 地址,只要连接某个以太网的两个路由器接口中有一个接口能够正常工作,该虚拟 IP 地址被自动映射到正常工作的路由器接口的 IP 地址,因此两个路由器互为备份,且终端对路由器之间的切换是透明的。

由于 Packet Tracer 中的路由器不支持 HSRP,因此在某个路由器丧失工作能力后,如果终端配置的默认网关地址恰好是该路由器接口的 IP 地址,需要将终端的默认网关地址重新配置成仍然具有工作能力的路由器接口的 IP 地址,否则该终端无法和其他网络中

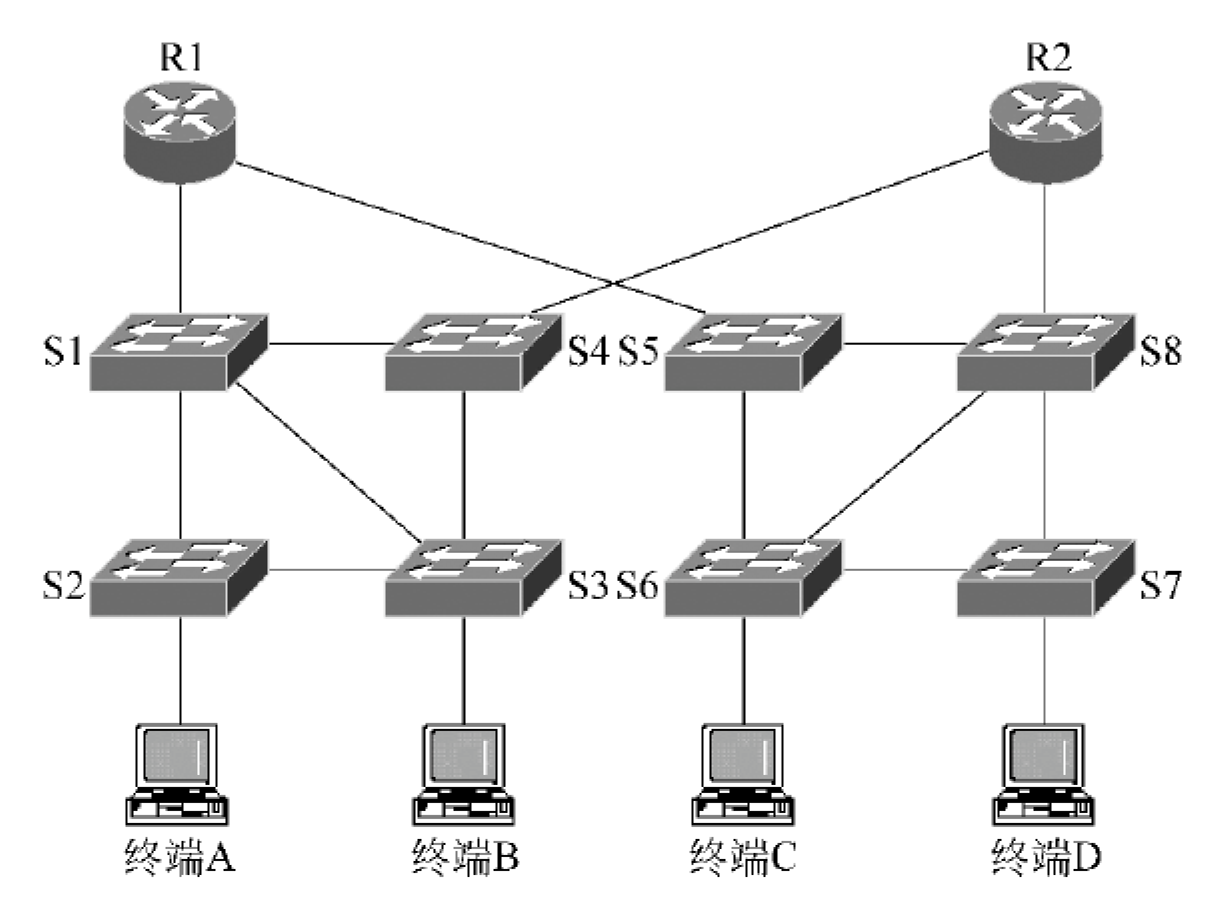


图 6.19　容错网络结构

的终端通信。这意味着终端必须手工完成第一跳路由器的切换。

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 6.19 所示的网络结构放置和连接设备，逻辑工作区完成设备放置和连接后的界面如图 6.20 所示。交换机 Switch1～Switch4 和 Switch5～Switch8 构成两个独立以太网，由于每一个独立以太网的交换机之间存在环路，生成树协议通过阻塞一些端口来消除交换机之间的环路。图 6.20 中标出了生成树协议最终阻塞的交换机端口。

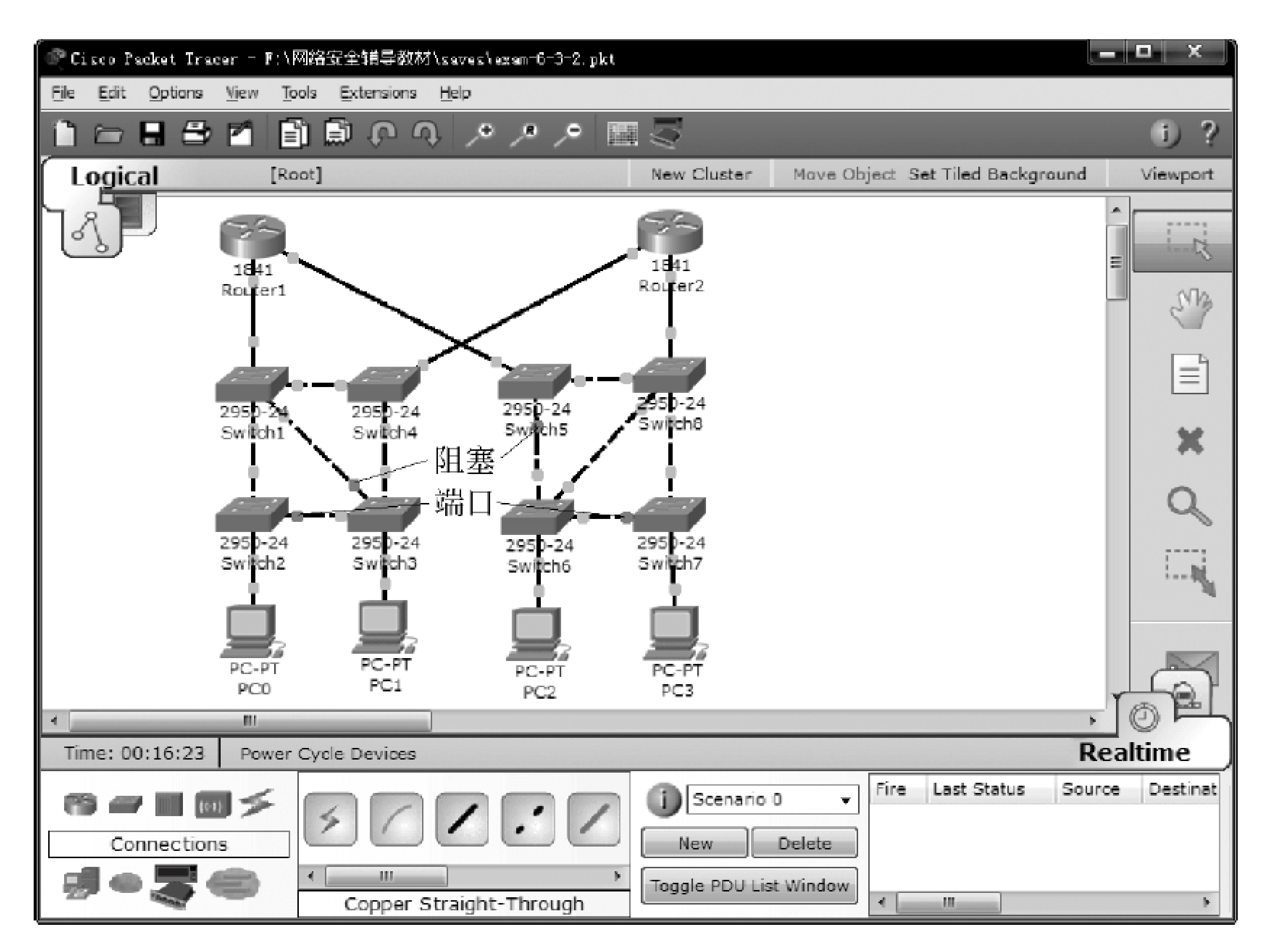


图 6.20　放置和连接设备后的逻辑工作区界面及被生成树协议阻塞的端口

（2）为路由器接口配置 IP 地址和子网掩码，连接在同一个以太网的路由器接口需配置网络号相同、主机号不同的 IP 地址。为终端配置网络信息，每一个终端可以在连接终端所在网络的两个路由器接口中任选一个接口的 IP 地址作为默认网关地址。图 6.21～图 6.24 表示两个网络中的终端均选择路由器 Router1 连接各自所在网络的接口的 IP 地址作为默认网关地址。完成配置后，同一网络的两个终端之间，不同网络的两个终端之间可以相互通信。

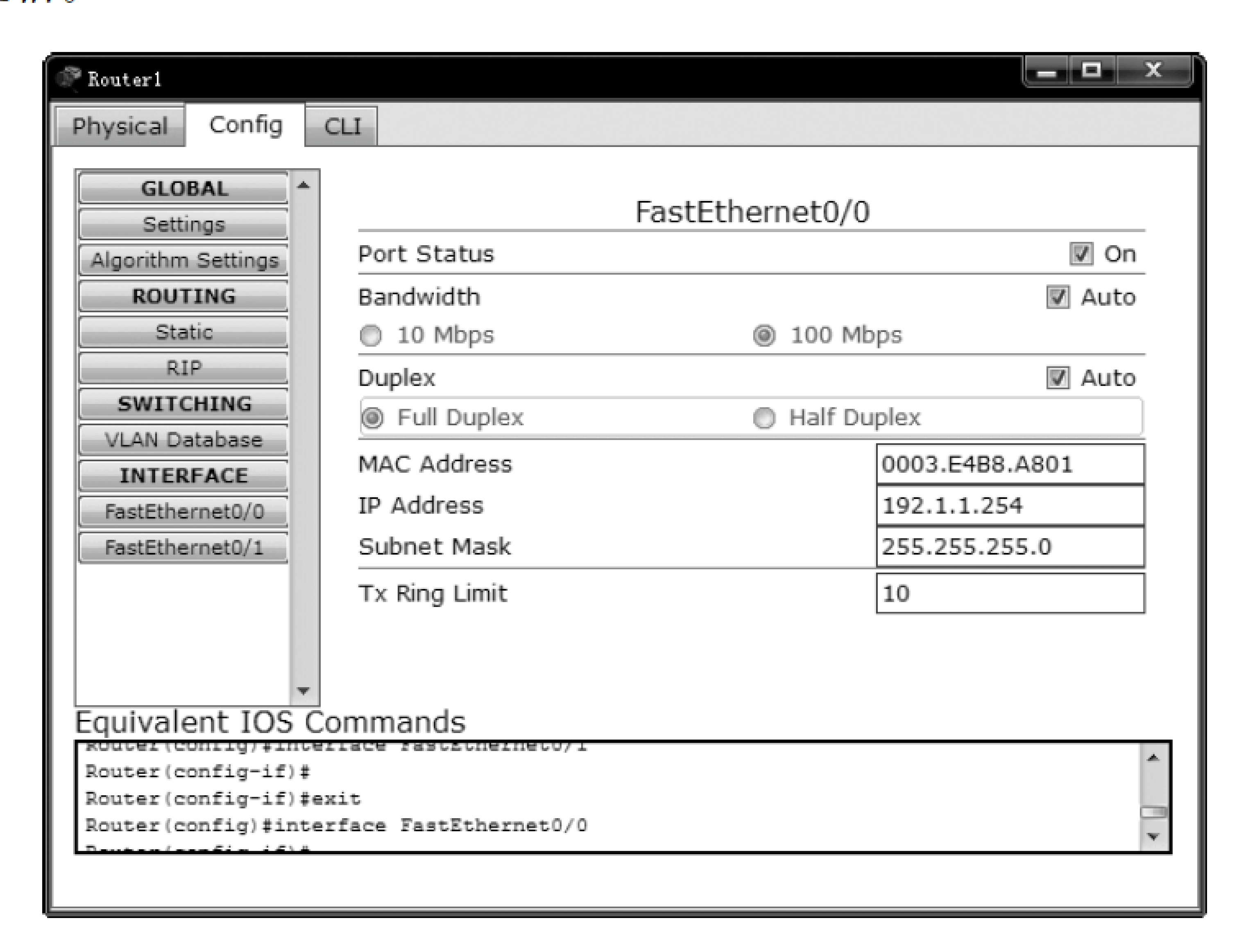


图 6.21　Router1 FastEthernet0/0 接口配置界面

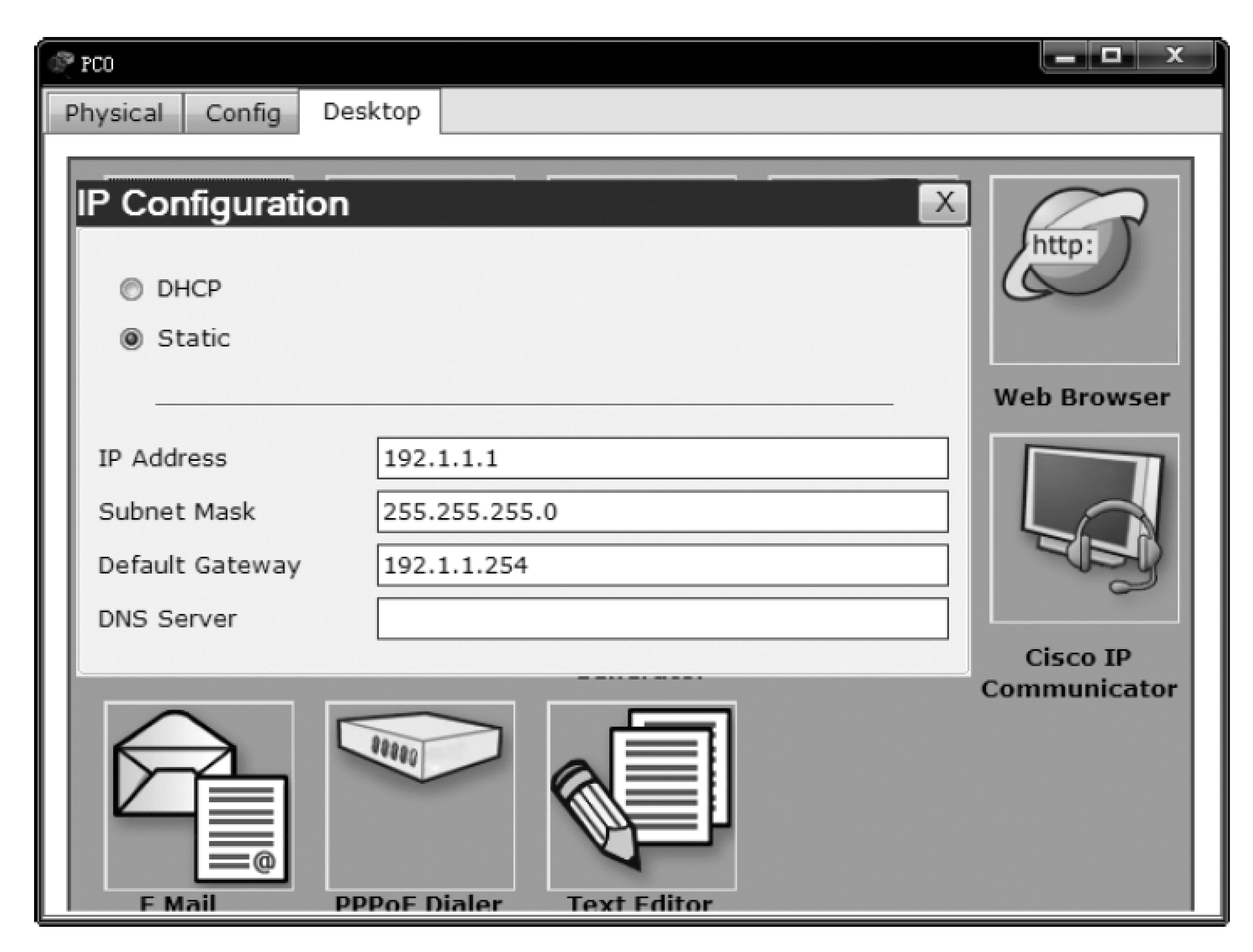


图 6.22　PC0 网络信息配置界面

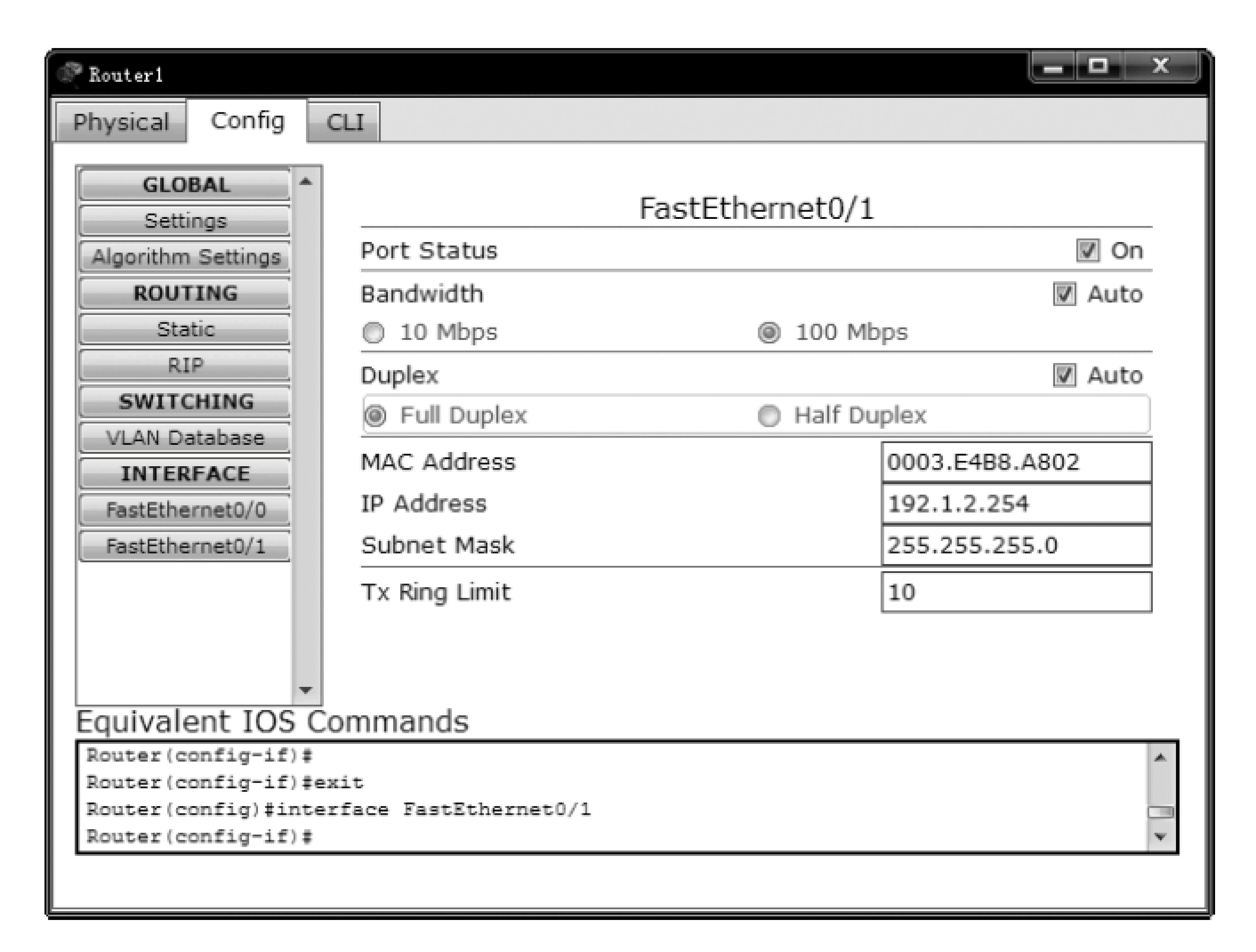


图 6.23 Router1 FastEthernet0/1 接口配置界面

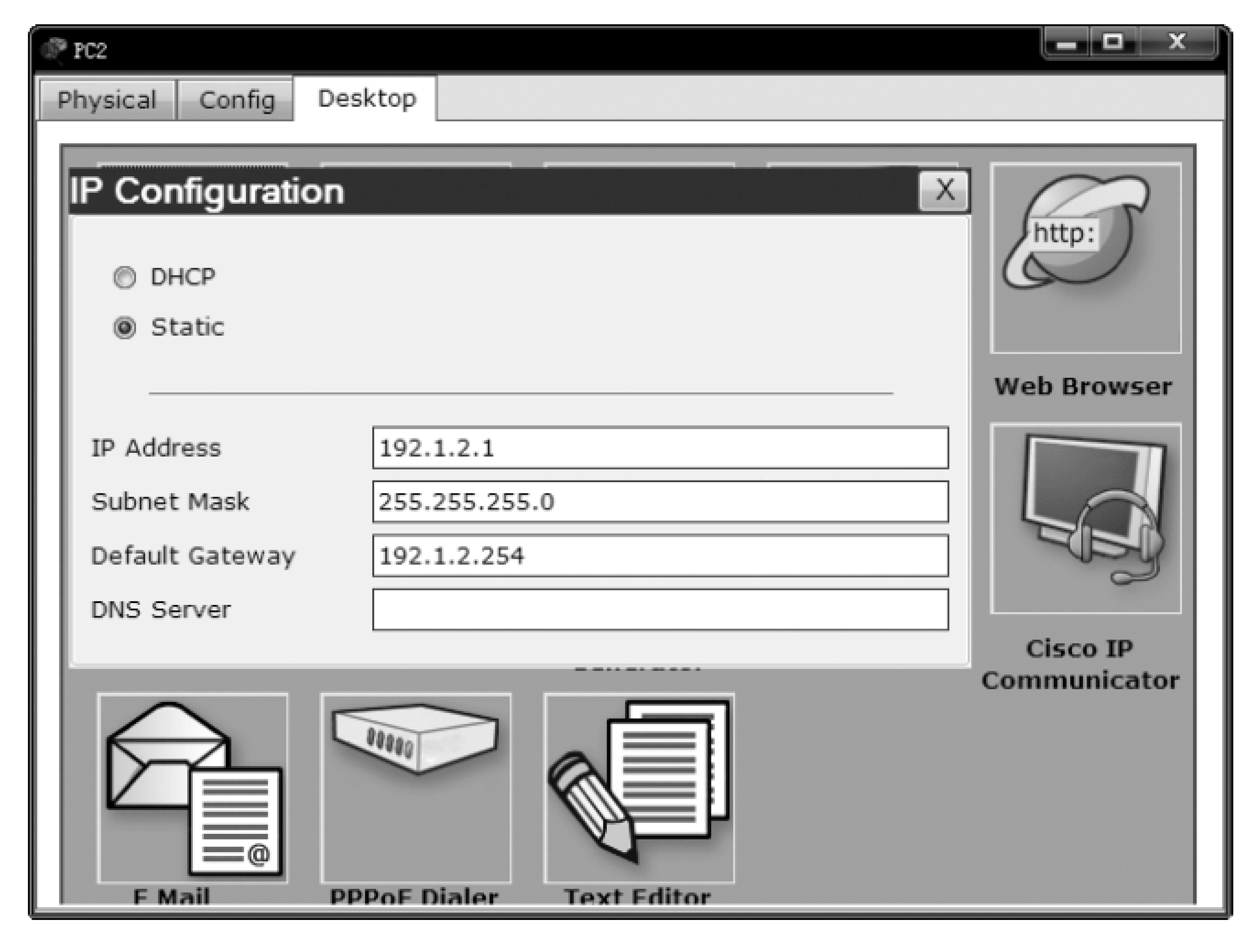


图 6.24 PC2 网络信息配置界面

(3) 在 Switch4 和 Switch8 及所连接的链路损坏的情况下,仍然能够保持同一网络的两个终端之间,不同网络的两个终端之间的连通性。图 6.25 给出了 Switch4 和 Switch8 及所连接的链路损坏后的网络结构,以及生成树协议重新生成的交换机端口状态。

(4) 如果发生路由器 Router1 及所连接的链路损坏的情况,如图 6.26 所示。由于两个网络中的终端均选择路由器 Router1 连接各自所在网络的接口的 IP 地址作为默认网关地址,因此,无法实现不同网络的终端之间通信,必须将两个网络中的终端的默认网关地址改为 Router2 连接各自所在网络的接口的 IP 地址后,才能重新恢复不同网络的终端之间的通信。这是手动切换终端第一跳路由器带来的不便。

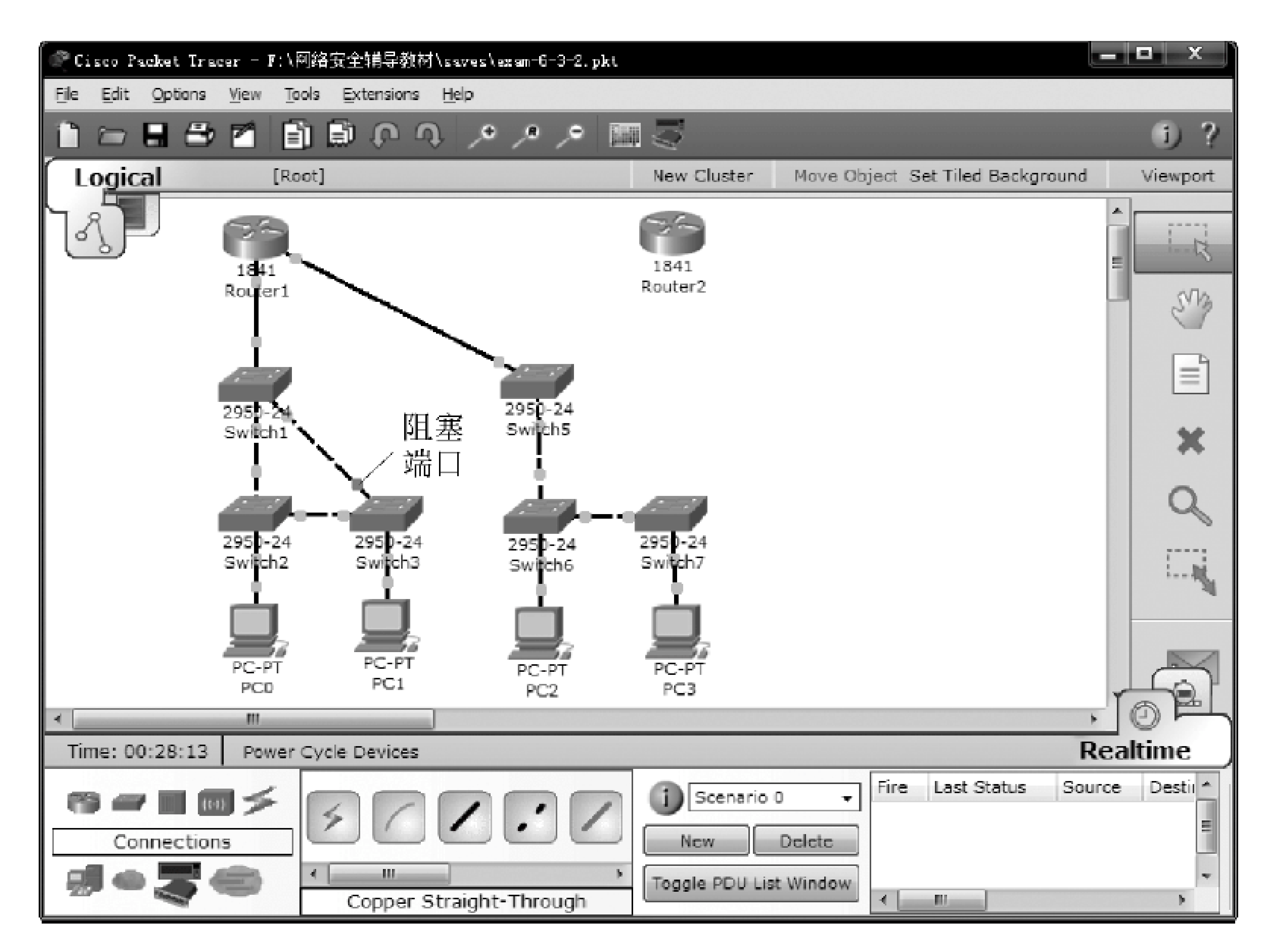


图 6.25　Switch4 和 Switch8 及所连接链路损坏后仍保持网络连通性

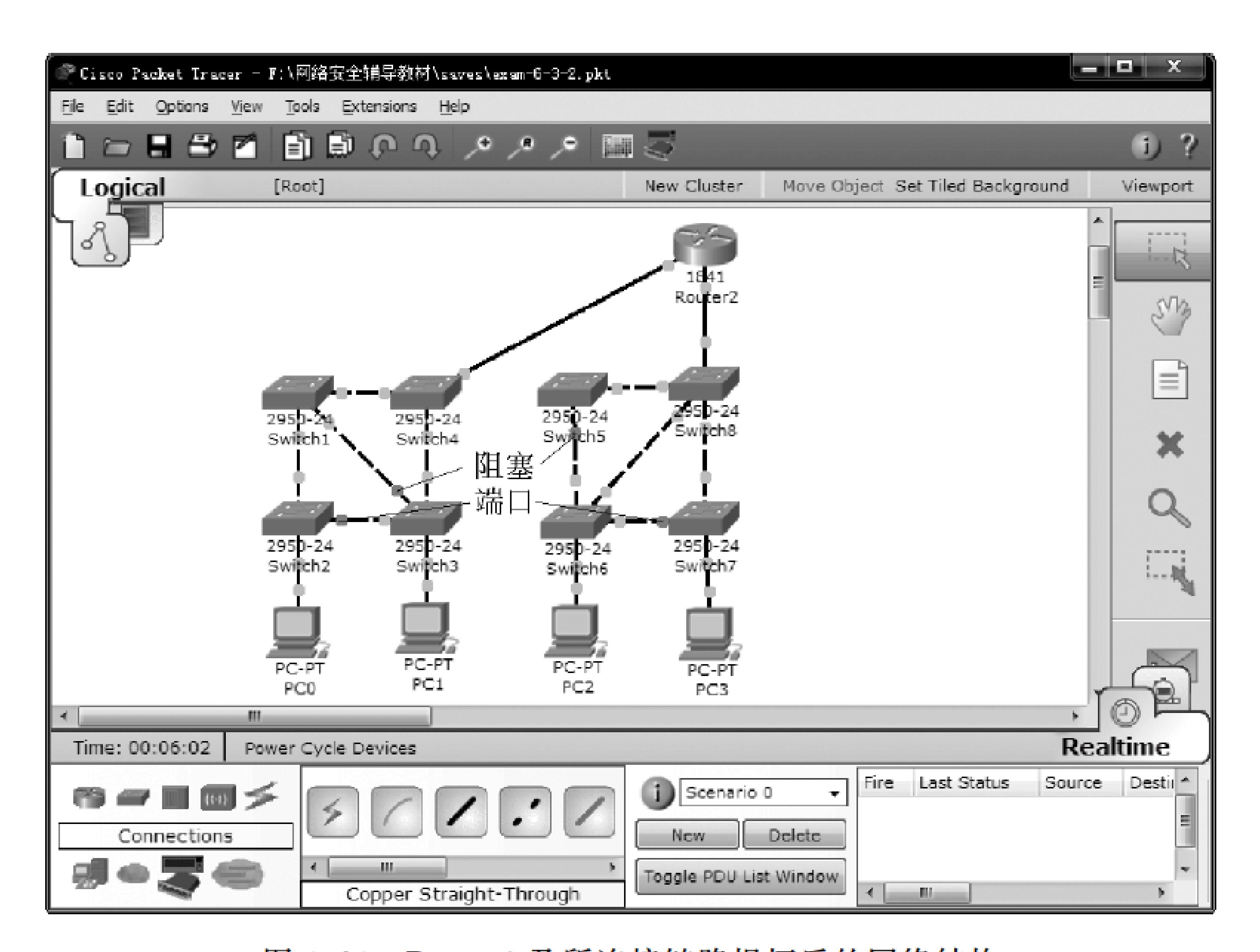


图 6.26　Router1 及所连接链路损坏后的网络结构

6.3.3　PAT 实验

1. 实验内容

(1) 完成网络设计和配置。

(2) 完成路由器 PAT 配置。

(3) 完成静态端口映射。

(4) 验证内部网络之间的连通性。

2. 网络结构

如图 6.27 所示,两个内部网络(内部网络 1 和内部网络 2)通过公共传输网络互连,这两个内部网络完全独立,因此可以分配相同的私有地址,图 6.27 中两个内部网络的私有地址都是 192.168.1.0/24 和 192.168.2.0/24。内部网络中的终端可以访问公共资源,但需要通过端口地址转换(Port Address Translation,PAT)技术将私有地址转换成边缘路由器 R1 和 R3 连接公共网络的接口的 IP 地址,用内部网络唯一的端口号标识内部网络终端的私有地址。允许两个内部网络中的终端共享两个内部网络中的 Web 服务器,即允许内部网络 1 中的终端 A 和终端 B 访问内部网络 2 中的 Web 服务器 2,允许内部网络 2 中的终端 C 和终端 D 访问内部网络 1 中的 Web 服务器 1,必须通过设置扩展过滤器禁止公共网络中的终端访问内部网络中的 Web 服务器。同样,允许两个内部网络中的终端访问内部网络 1 中的 E-mail 服务器 1,为了和公共网络中的 E-mail 服务器 2 交换邮件,允许 E-mail 服务器 1 和 E-mail 服务器 2 交换 SMTP 报文,但必须通过设置扩展过滤器禁止公共网络中的终端访问内部网络 1 中的 E-mail 服务器 1。

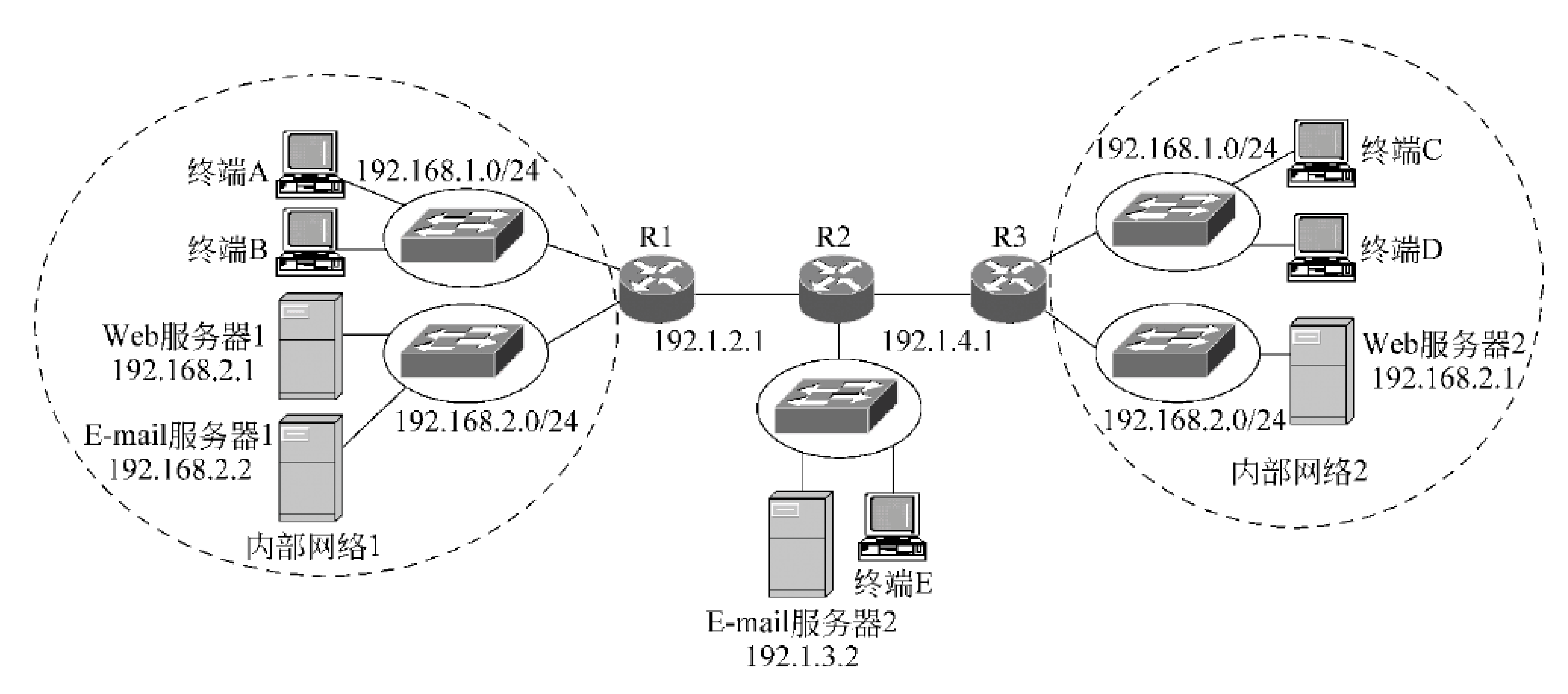


图 6.27 PAT 实现过程

原始状态下,内部网络对于公共网络是不可见的,因此公共网络中的终端无法发起访问内部网络资源的过程。这也导致某个内部网络中的终端只能发起访问公共网络资源的过程,无法发起访问另一个内部网络中资源的过程,即某个内部网络对另一个内部网络也是不可见的,这是允许两个内部网络分配的私有 IP 地址重叠的原因。为实现一个内部网络中的终端发起访问另一个内部网络中的服务器的访问过程,必须静态建立内部网络中唯一的端口号与该服务器私有 IP 地址之间的映射,这样可以用该内部网络边缘路由器的全球 IP 地址和与内部网络中服务器私有 IP 地址绑定的内部网络中唯一的端口号访问该内部网络中的服务器。

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 6.27 所示的网络结构放置和连接设备，逻辑工作区完成设备放置和连接后的界面如图 6.28 所示。

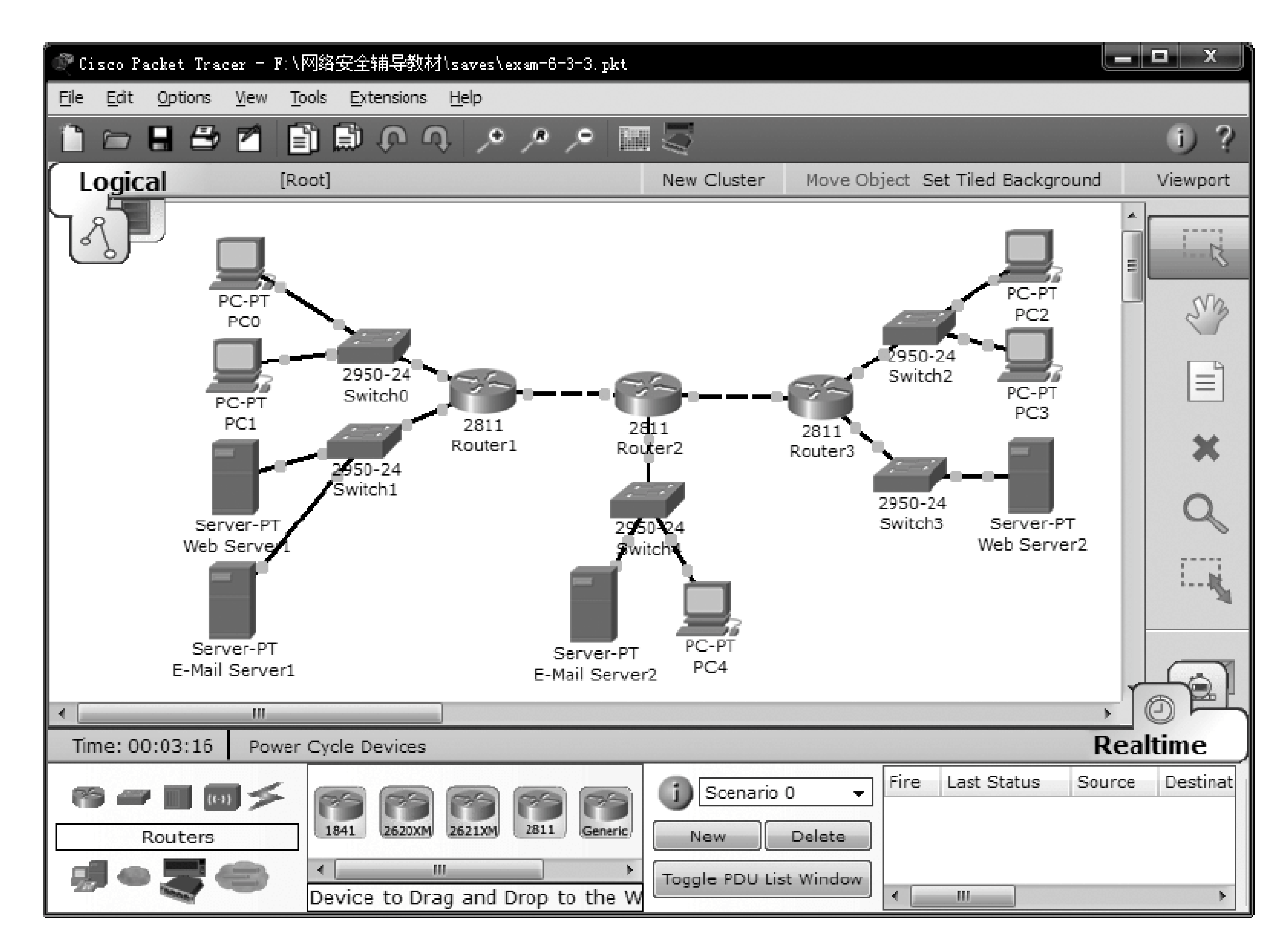


图 6.28　放置和连接设备后的逻辑工作区界面

(2) 配置各个路由器接口的 IP 地址和子网掩码，启动各个路由器的 RIP 进程，配置参与建立 RIP 动态路由项的网络。值得指出的是，Router1 和 Router3 中内部网络 192.168.1.0/24和 192.168.2.0/24 不参与 RIP 动态路由项的建立过程，因此对于 Router2，内部网络是透明的，同样，Router1 和 Router3 也只知道与其直接相连的内部网络。图 6.29～图 6.31 所示的 Router1～Router3 路由表内容充分表明了这一点。

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet1/0	---	0/0
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0
R	192.1.3.0/24	FastEthernet1/0	192.1.2.2	120/1
R	192.1.4.0/24	FastEthernet1/0	192.1.2.2	120/1

图 6.29　Router1 路由表

Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet0/0	---	0/0
C	192.1.3.0/24	FastEthernet1/0	---	0/0
C	192.1.4.0/24	FastEthernet0/1	---	0/0

图 6.30　Router2 路由表

Routing Table for Router3

Type	Network	Port	Next Hop IP	Metric
C	192.1.4.0/24	FastEthernet1/0	---	0/0
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0
R	192.1.2.0/24	FastEthernet1/0	192.1.4.2	120/1
R	192.1.3.0/24	FastEthernet1/0	192.1.4.2	120/1

图 6.31 Router3 路由表

(3) Router1 和 Router3 中启动 PAT 功能，分别以 Router1 和 Router3 连接公共网络的接口的 IP 地址为内部网络终端发送到公共网络上的 IP 分组的源 IP 地址，如 Router1 通过命令“ip nat inside source list 1 interface FastEthernet1/0 overload”指定将编号为 1 的标准过滤器规定的私有 IP 地址转换成接口 FastEthernet1/0 配置的全球 IP 地址。因此，内部网络 1 中终端发送的 IP 分组进入公共网络后，源 IP 地址为 Router1 接口 FastEthernet1/0 的 IP 地址 192.1.2.1。内部网络 2 中终端发送的 IP 分组进入公共网络后，源 IP 地址为 Router3 连接 Router2 的接口的 IP 地址 192.1.4.1。为了允许一个内部网络中的终端访问另一个内部网络中的 Web 服务器，必须静态配置内部网络内唯一的端口号与该 Web 服务器的私有 IP 地址之间的绑定，如 Router1 用命令“ip nat inside source static tcp 192.168.2.1 80 192.1.2.1 80”建立 192.1.2.1:80 与 192.168.2.1:80 的静态映射。这样，其他网络(包括公共网络和其他内部网络)中的终端可以通过 URL=192.1.2.1:80(端口号 80 允许省略)访问内部网络 1 中的 Web 服务器 1。图 6.32 是 PC0 配置的内部网络的网络信息。图 6.33 是 PC0 访问内部网络 2 中 Web 服务器 2 的界面，前提是 Router3 已经建立 192.1.4.1:80 与 192.168.2.1:80 的静态映射。

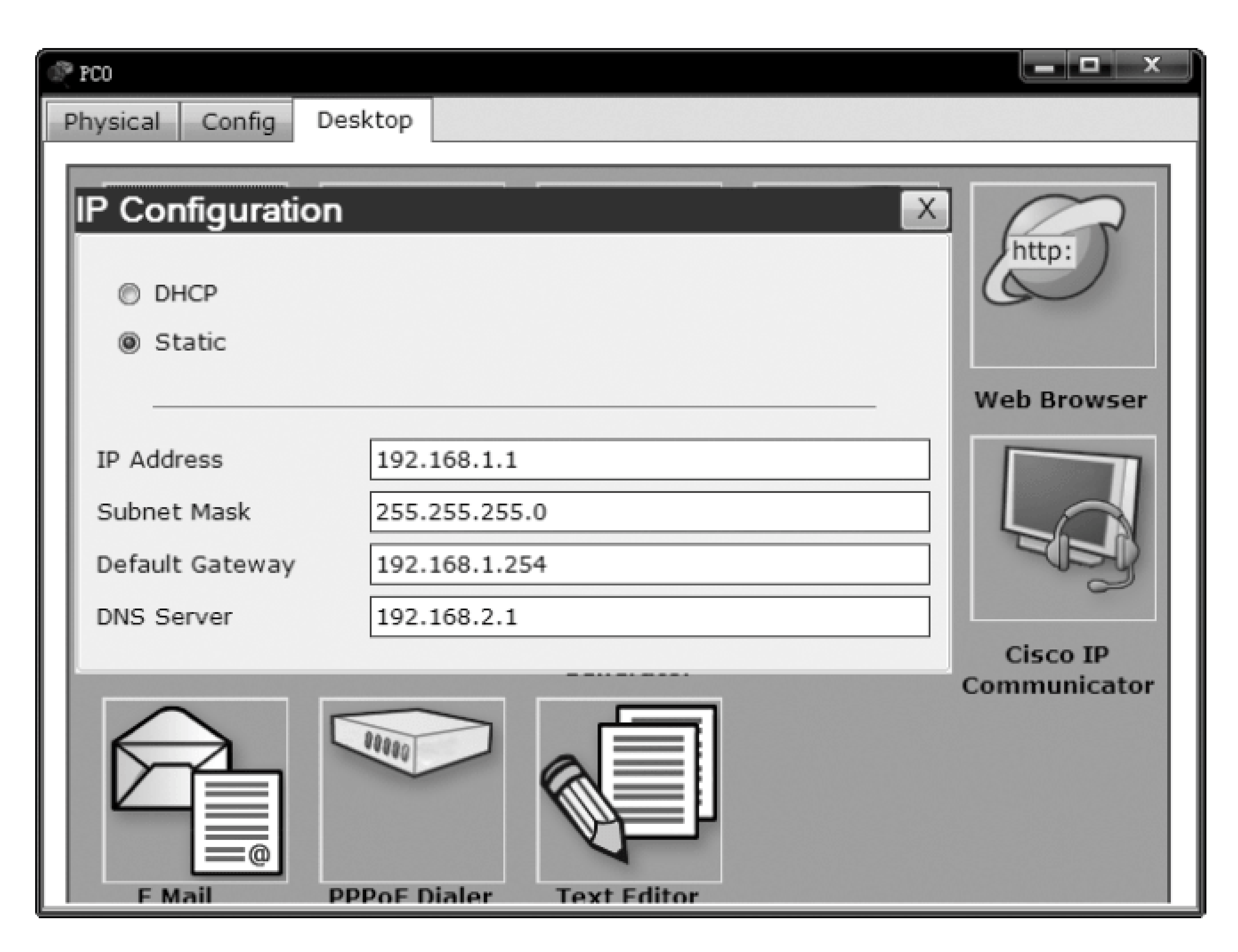


图 6.32 PC0 配置的网络信息

(4) 如果只允许内部网络中的终端访问内部网络中的 Web 服务器，必须在 Router1 和 Router3 连接内部网络 192.168.2.0/24 的接口的输出方向上设置扩展过滤器，只允许

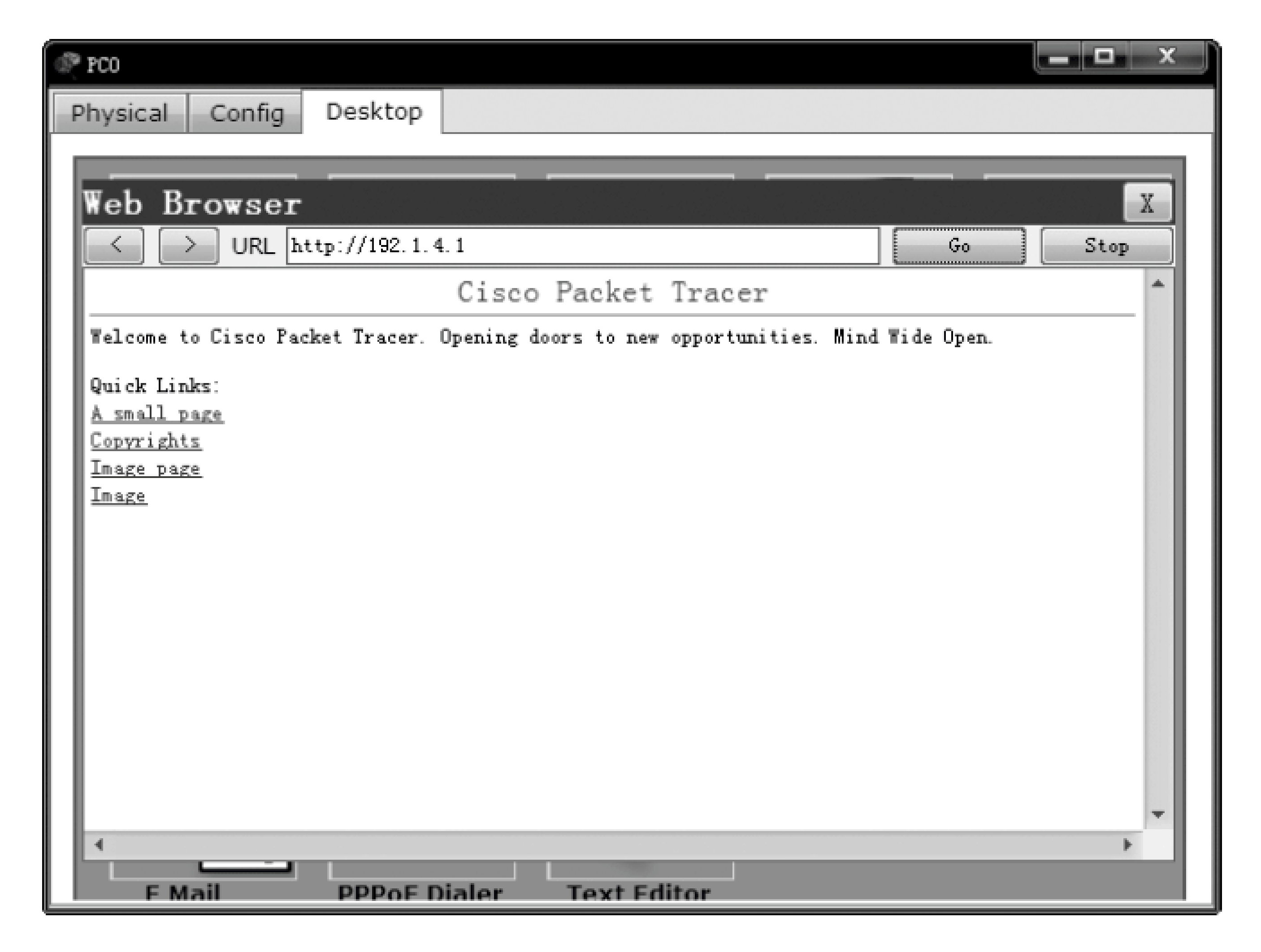


图 6.33　PC0 访问 Web 服务器 2 的界面

与内部网络中的终端访问 Web 服务器相关的 TCP 报文进入网络 192.168.2.0/24，Router1 通过过滤规则"access-list 101 permit tcp host 192.1.4.1 host 192.168.2.1 eq www"表明了这一点。其中 192.1.4.1 是所有内部网络 2 中终端发送的 IP 分组到达 Router1 时的源 IP 地址。如果 Router3 用过滤规则"access-list 101 permit tcp host 192.1.2.1 host 192.168.2.1 eq www "表明只允许源 IP 地址为 192.1.2.1（所有内部网络 1 中终端发送的 IP 分组到达 Router3 时的源 IP 地址）的 IP 分组进入网络 192.168.2.0/24，PC4 发送的 IP 分组由于源地址为 192.1.3.1，被 Router3 丢弃。图 6.34 是 PC4 配置的网络信息。图 6.35 是 PC4 访问内部网络 2 中 Web 服务器 2 失败的界面。

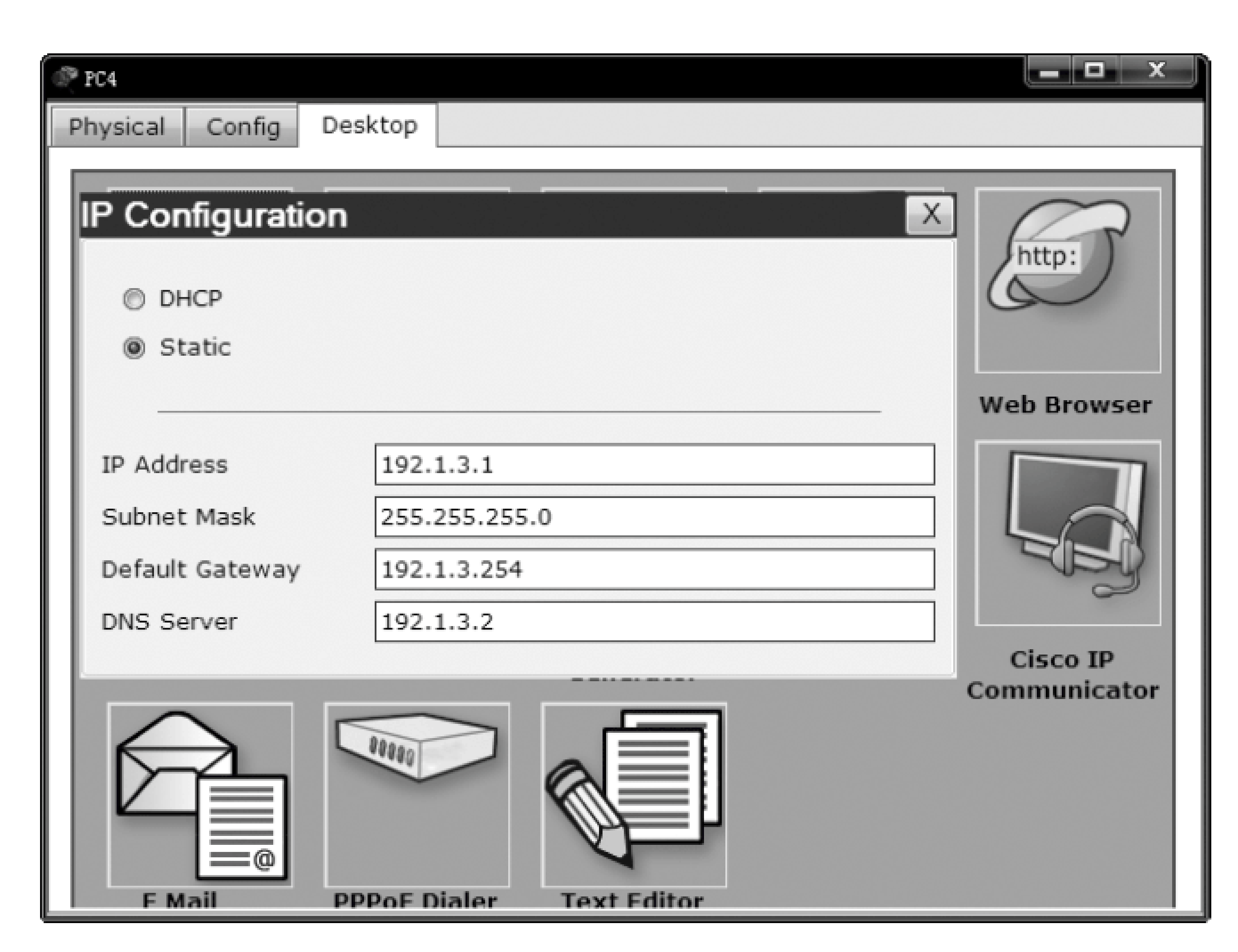


图 6.34　PC4 配置的网络信息



图 6.35 PC4 访问 Web 服务器 2 失败的界面

(5) PC0、PC1 访问内部网络 2 中的 Web 服务器 2,PC2、PC3 访问内部网络 1 中的 Web 服务器 1 后,Router1 和 Router3 建立图 6.36 和图 6.37 所示的 NAT 表。表中存在两种内部本地信息和内部全球信息之间的映射:一种是静态映射,如 Router1 中的 192.1.2.1:80(内部全球信息)和 192.168.2.1:80(内部本地信息),将源 IP 地址和源端口号为 192.168.2.1:80 的 IP 分组转换成源 IP 地址和源端口为 192.1.2.1:80 的 IP 分组后,从内部网络输出到公共网络,反之,将目的 IP 地址和目的端口号为 192.1.2.1:80 的 IP 分组转换成目的 IP 地址和目的端口号为 192.168.2.1:80 的 IP 分组后,从公共网络输入到内部网络。一种是动态映射,如 Router1 中 PC0 和 PC1 访问内部网络 2 中的 Web 服务器 2 产生的动态映射 192.1.2.1:1024(内部全球信息)与 192.168.1.2:1025(内部本地信息)和 192.1.2.1:1025(内部全球信息)与 192.168.1.1:1025(内部本地信息),这里 PC0 和 PC1 发送的 TCP 报文的源 IP 地址都被转换成全球 IP 地址 192.1.2.1,内部网络 2 中 Web 服务器 2 向 PC0 和 PC1 发送的 TCP 报文的目的 IP 地址均是 192.1.2.1,Router1 为了能够将目的 IP 地址相同的 TCP 报文转发给不同的内部网络终端,用内部网络唯一的源端口绑定内部网络终端的私有 IP 地址,因此用源端口号 1025 绑定私有 IP 地址 192.168.1.1 后,必须用不同的源端口号 1024 绑定私有 IP 地址 192.168.1.2。尽管 PC1 选择的源端口号也是 1025,Router1 必须用内部网络中唯一的源端口 1024 取代原来的源端口 1025。动态映射中外部本地信息和外部全球信息是相同的,指的是内部网络终端访问的 Web 服务器在公共网络中使用的信息。

NAT Table for Router1

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
tcp	192.1.2.1:1024	192.168.1.2:1025	192.1.4.1:80	192.1.4.1:80
tcp	192.1.2.1:1025	192.168.1.1:1025	192.1.4.1:80	192.1.4.1:80
tcp	192.1.2.1:110	192.168.2.2:110	---	---
tcp	192.1.2.1:25	192.168.2.2:25	---	---
tcp	192.1.2.1:80	192.168.2.1:80	---	---
tcp	192.1.2.1:80	192.168.2.1:80	192.1.4.1:1024	192.1.4.1:1024
tcp	192.1.2.1:80	192.168.2.1:80	192.1.4.1:1025	192.1.4.1:1025

图 6.36 Router1 NAT 表

NAT Table for Router3

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
tcp	192.1.4.1:1024	192.168.1.2:1025	192.1.2.1:80	192.1.2.1:80
tcp	192.1.4.1:1025	192.168.1.1:1025	192.1.2.1:80	192.1.2.1:80
tcp	192.1.4.1:80	192.168.2.1:80	---	---
tcp	192.1.4.1:80	192.168.2.1:80	192.1.2.1:1024	192.1.2.1:1024
tcp	192.1.4.1:80	192.168.2.1:80	192.1.2.1:1025	192.1.2.1:1025

图 6.37　Router3 NAT 表

（6）为了允许内部网络中的终端通过内部网络 1 中的 E-mail 服务器 1 发送、接收邮件，必须允许内部网络 2 的终端通过 SMTP 和 POP3 访问内部网络 1 中的 E-mail 服务器 1。为了允许内部网络 1 中的 E-mail 服务器 1 和公共网络中的 E-mail 服务器 2 交换邮件，必须允许这两个 E-mail 服务器通过 SMTP 访问对方。为此，Router1 通过命令“ip nat inside source static tcp 192.168.2.2 110 192.1.2.1 110”和“ip nat inside source static tcp 192.168.2.2 25 192.1.2.1 25”建立 192.1.2.1:110 与 192.168.2.2:110、192.1.2.1:25 与 192.168.2.2:25 的静态映射，这里 110 是 POP3 对应的著名端口号，25 是 SMTP 对应的著名端口号。Router1 通过在连接内部网络 192.168.2.0/24 的接口的输出方向上设置扩展过滤器指定允许到达内部网络 1 中的 E-mail 服务器 1 的 TCP 报文范围。

（7）如果将内部网络 E-mail 服务器的域名设置为 163.COM，公共网络 E-mail 服务器的域名设置为 263.COM，需要在内部网络 1、内部网络 2 和公共网络中配置域名服务器。与域名 263.COM 绑定的 IP 地址，对所有网络中的终端都是相同的，固定为 192.1.3.2；对于内部网络 1 中的终端，与域名 163.COM 绑定的 IP 地址是其私有 IP 地址 192.168.2.2；对于内部网络 2 中的终端和公共网络中的 E-mail 服务器，与域名 163.COM 绑定的 IP 地址是全球 IP 地址 192.1.2.1。内部网络中的终端用 Web 服务器作为 DNS 服务器，Web 服务器 1 的 DNS 配置界面如图 6.38 所示，Web 服务器 2 的 DNS 配置界面如图 6.39 所示。

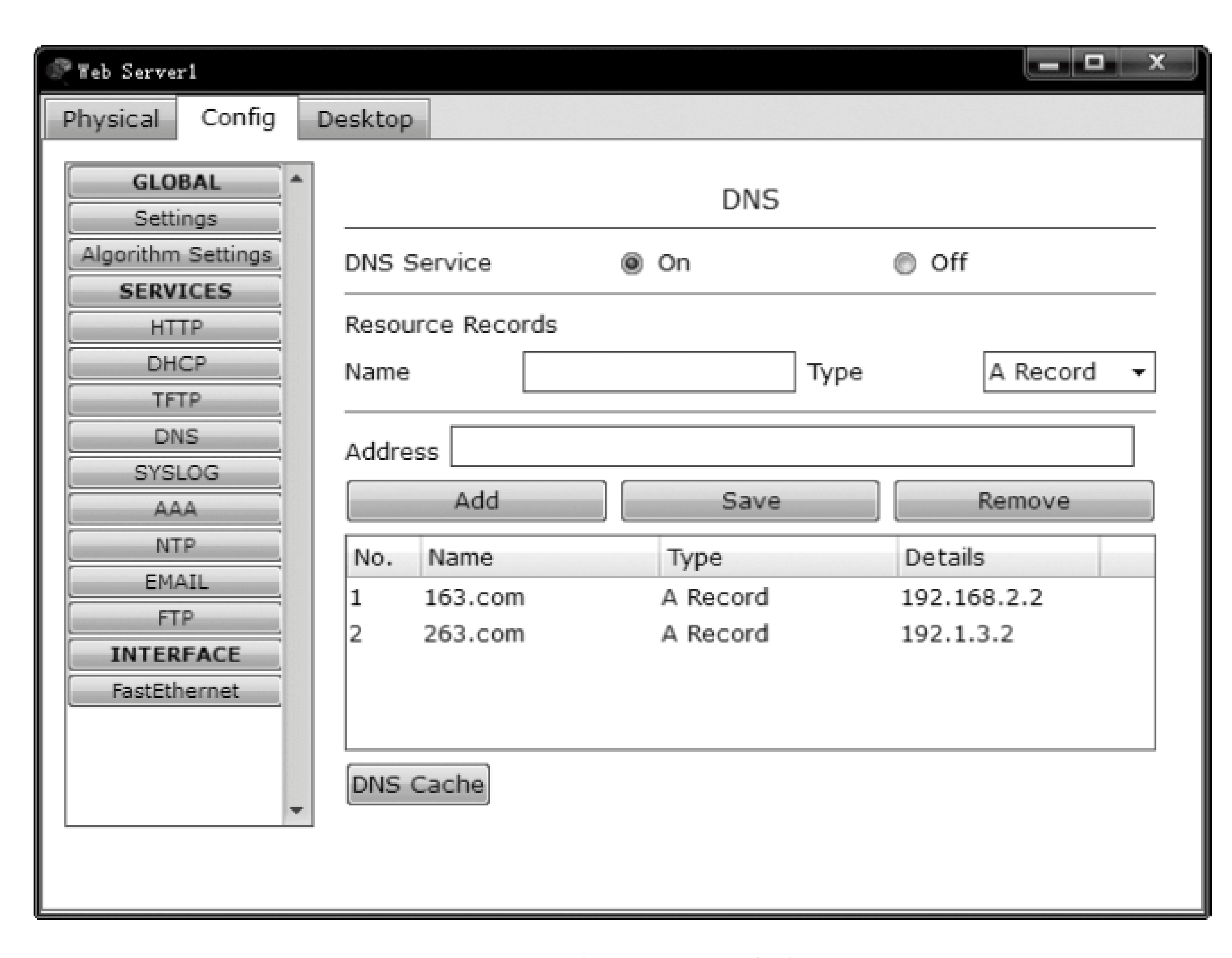


图 6.38　Web 服务器 1 的域名配置界面

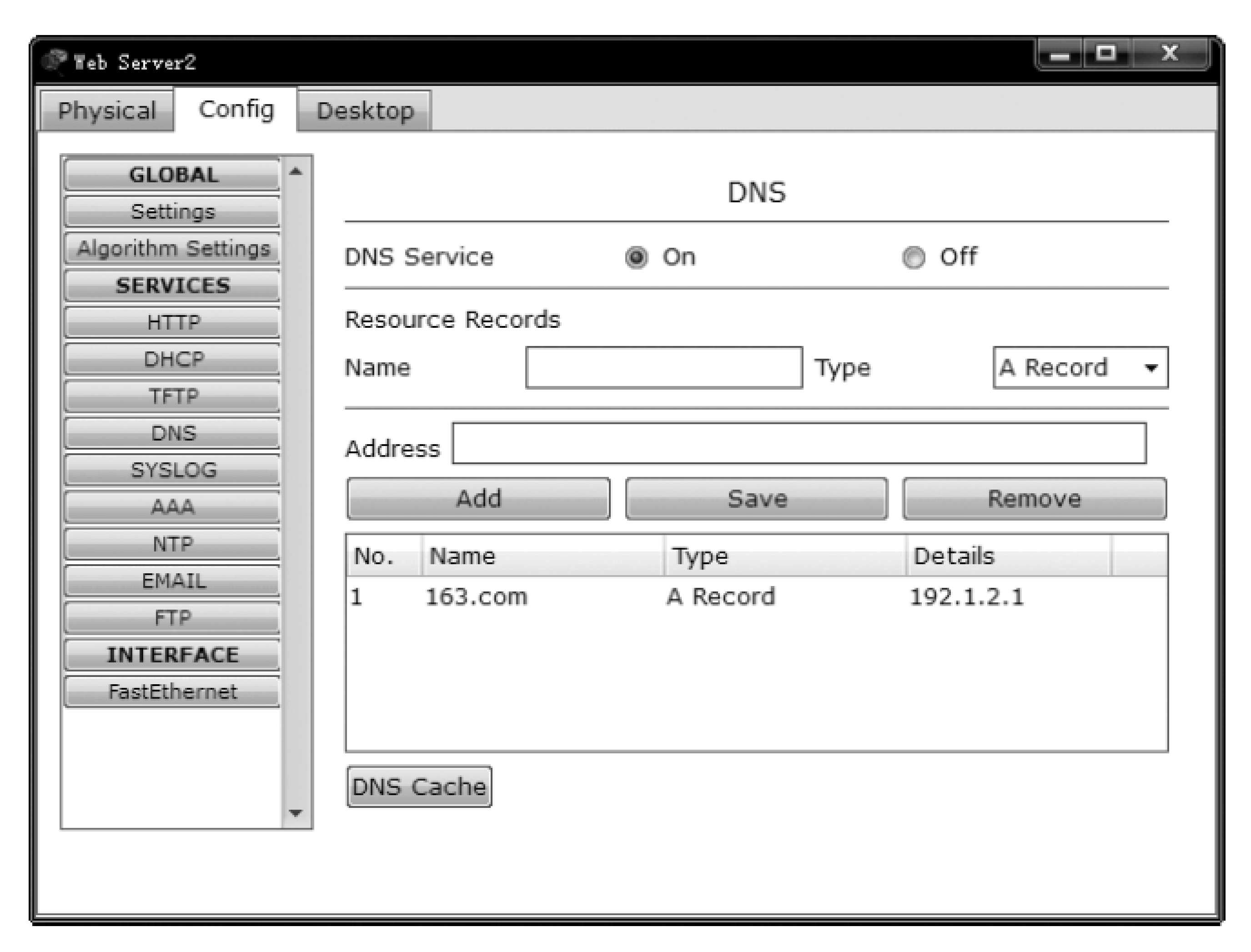


图 6.39　Web 服务器 2 的域名配置界面

（8）为了实现内部网络终端之间邮件发送和接收，需要在 E-mail 服务器 1 中创建用户。图 6.40 是创建用户 aaa1@163.COM 和 aaa2@163.COM 的界面。图 6.41 是 PC0 E-mail 实用程序的配置界面，图 6.42 是 PC0 收发邮件界面，图 6.43 是 PC0 编辑邮件界面。

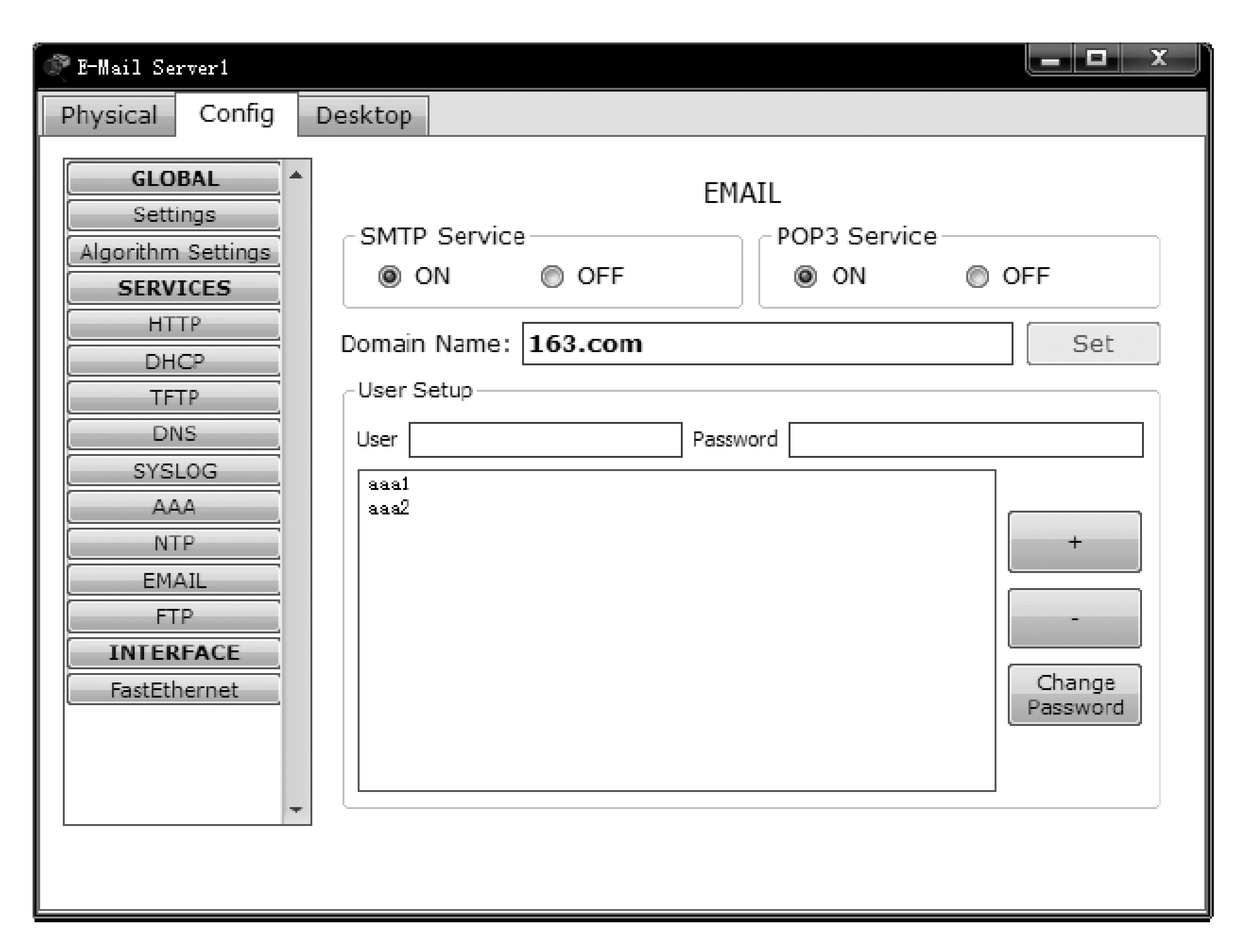


图 6.40　E-mail 服务器 1 注册用户界面

4. 命令行配置过程

（1）Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
```

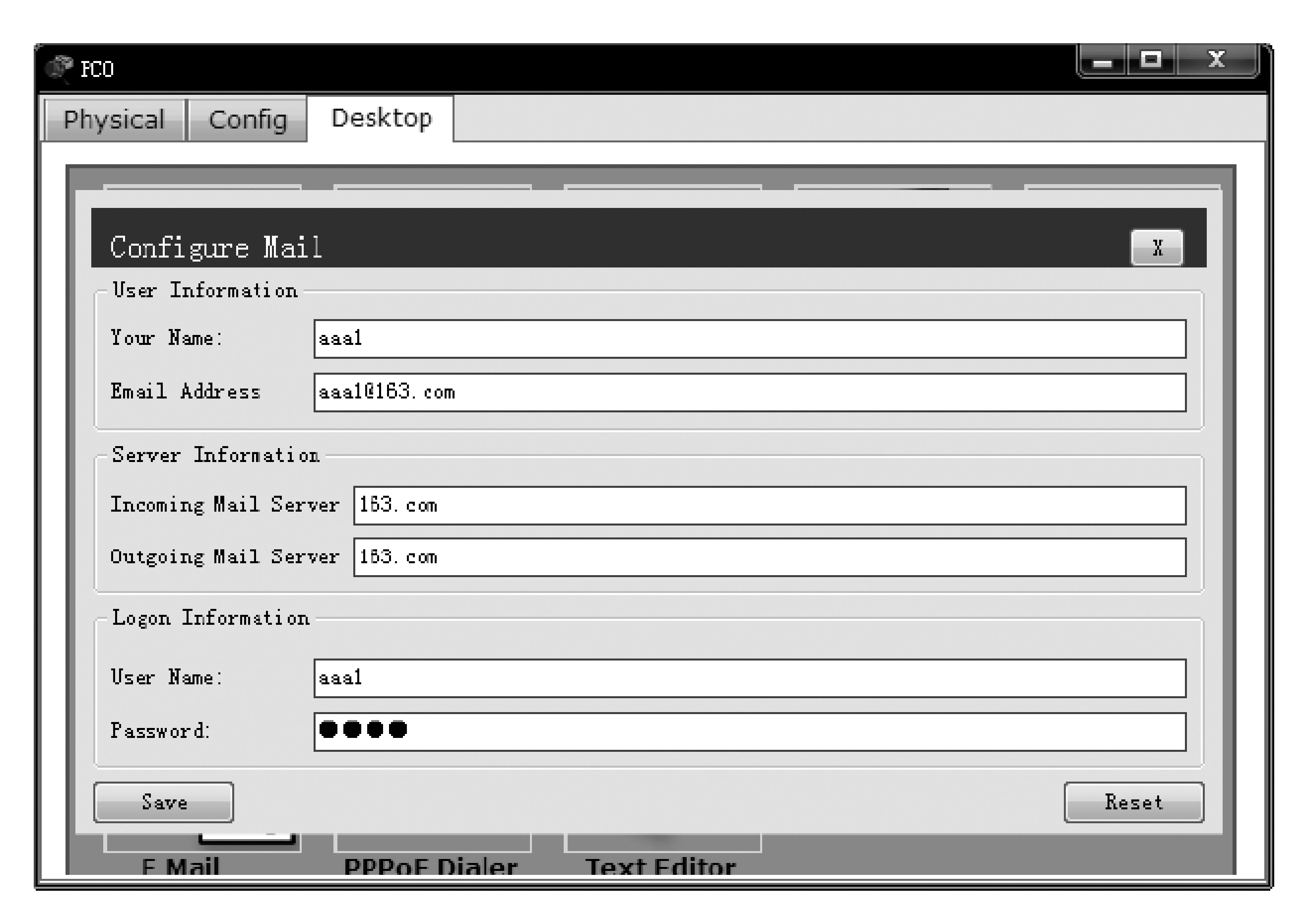


图 6.41　PC0 信箱配置界面

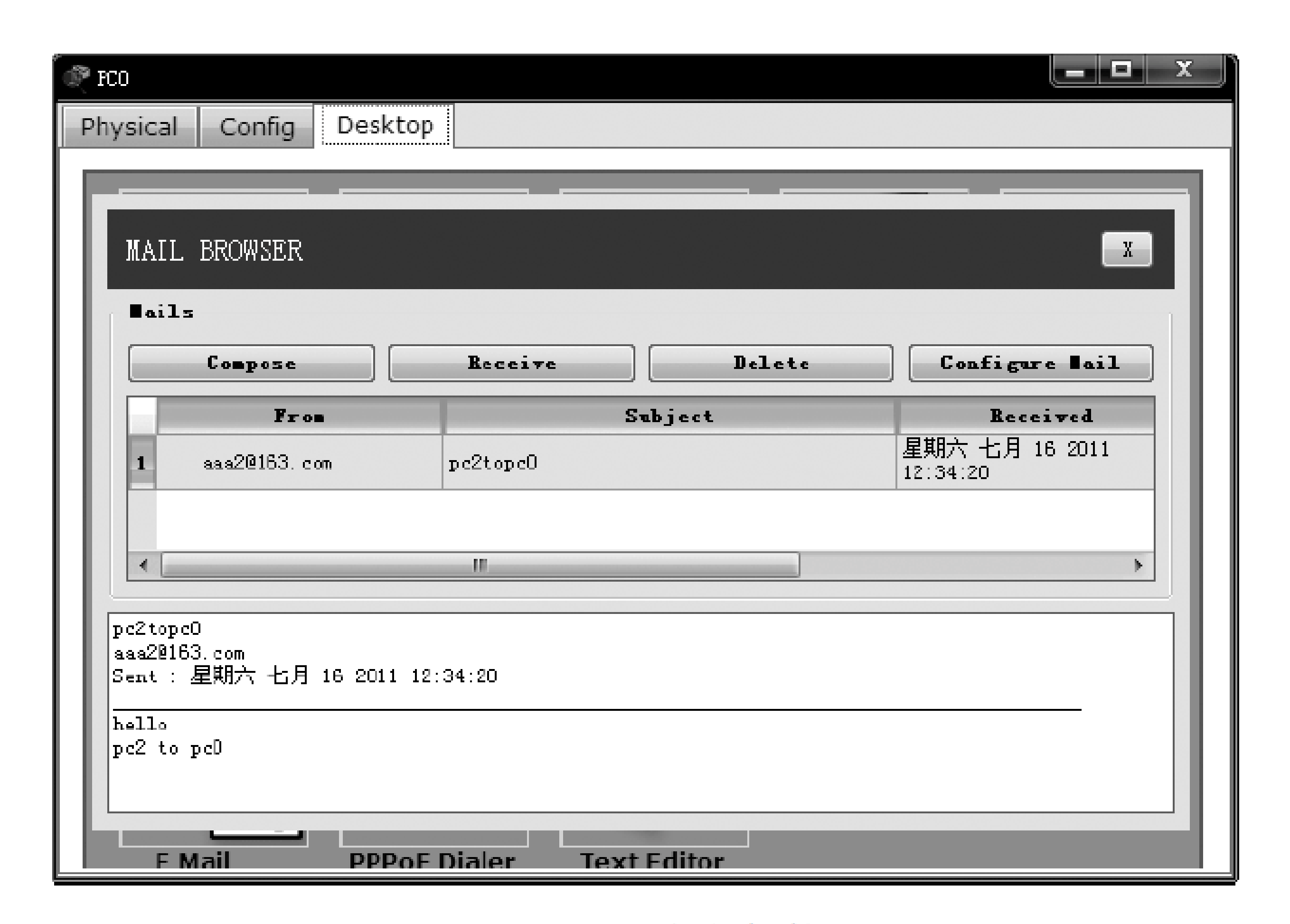


图 6.42　PC0 收发邮件界面

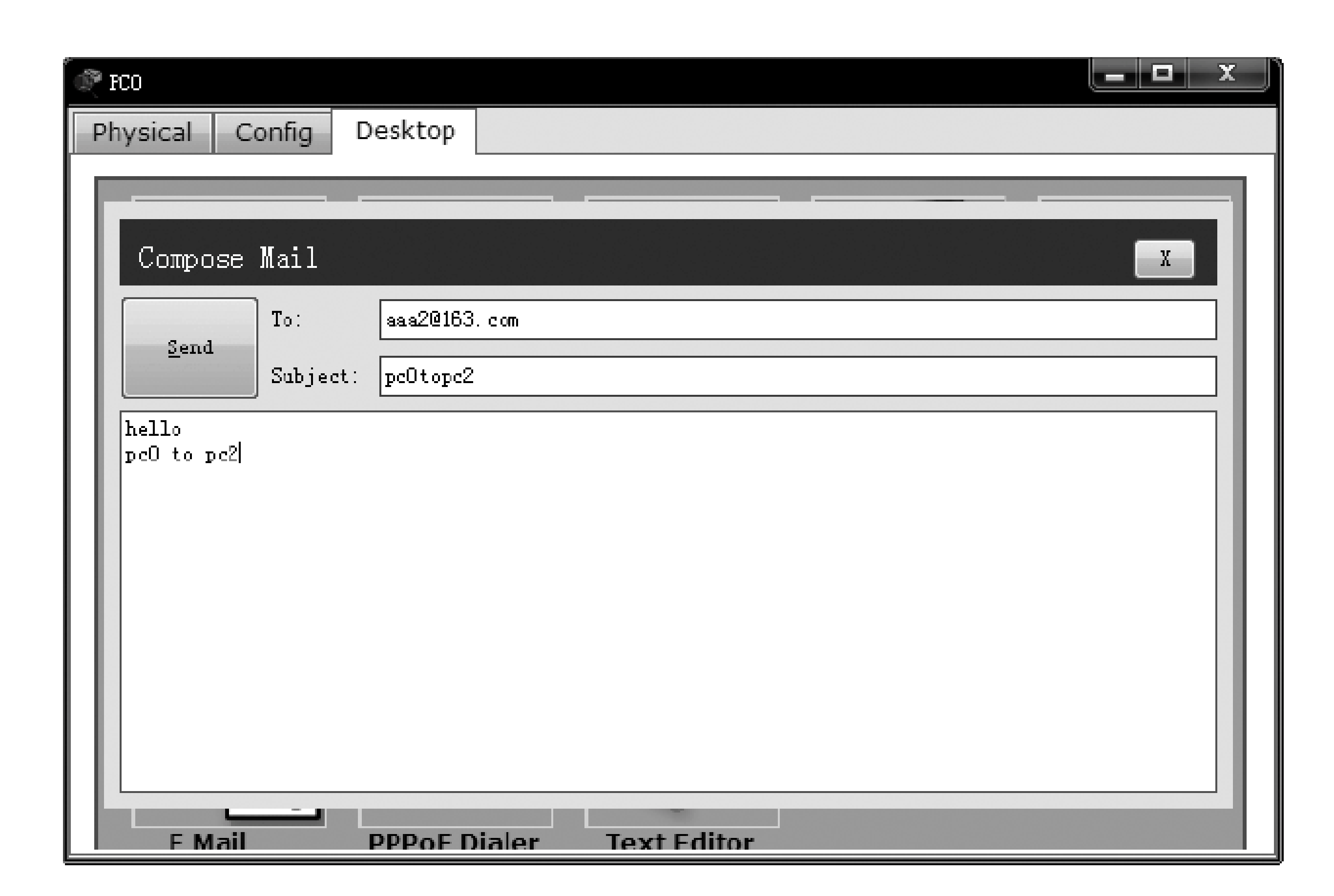


图 6.43　PC0 编辑邮件界面

```
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.1 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
                    (网络 192.1.2.0/24 及连接该网络的接口参与 RIP 动态路由项建立过程)
Router(config-router)#exit
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
                    (定义需要 NAT 的内部网络私有地址范围 192.168.1.0/24)
Router(config)#access-list 1 deny any
Router(config)#ip nat inside source list 1 interface FastEthernet1/0 overload
                    (允许编号为 1 的标准过滤器定义的内部网络私有地址与接口
                    FastEthernet1/0 的全球 IP 地址之间建立动态映射)
Router(config)#access-list 2 permit host 192.168.2.2
                    (定义需要 NAT 的内部网络主机地址 192.168.2.2/32)
Router(config)#access-list 2 deny any
Router(config)#ip nat inside source list 2 interface FastEthernet1/0 overload
                    (允许编号为 2 的标准过滤器定义的内部网络私有地址与接口
                    FastEthernet1/0 的全球 IP 地址之间建立动态映射)
Router(config)#ip nat inside source static tcp 192.168.2.1 80 192.1.2.1 80
    (建立内部网络服务器在内部网络使用的本地信息 192.168.2.1:80 与在公共网络使用的全球
    信息 192.1.2.1:80 之间的静态映射。全球信息中的端口号 80 必须是内部网络唯一的)
Router(config)#ip nat inside source static tcp 192.168.2.2 110 192.1.2.1 110
    (建立内部网络服务器在内部网络使用的本地信息 192.168.2.2:110 与在公共网络使用的全
    球信息 192.1.2.1:110 之间的静态映射。全球信息中的端口号 110 必须是内部网络唯一的)
Router(config)#ip nat inside source static tcp 192.168.2.2 25 192.1.2.1 25
    (建立内部网络服务器在内部网络使用的本地信息 192.168.2.2:25 与在公共网络使用的全球
    信息 192.1.2.1:25 之间的静态映射。全球信息中的端口号 25 必须是内部网络唯一的)
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside                 (指定连接内部网络接口)
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip nat inside                 (指定连接内部网络接口)
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip nat outside                (指定连接公共网络接口)
```

```
Router(config-if)#exit
Router(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 any
                    (允许源 IP 地址为 192.168.1.0/24 的 IP 分组继续转发的过滤规则)
Router(config)#access-list 101 permit tcp host 192.1.4.1 host 192.168.2.1 eq www
        (允许源 IP 地址为 192.1.4.1/32、目的 IP 地址为 192.168.2.1/32、目的端口号为 HTTP 对
        应的著名端口号的 TCP 报文继续转发的过滤规则)
Router(config)#access-list 101 permit tcp host 192.1.4.1 host 192.168.2.2 eq pop3
        (允许源 IP 地址为 192.1.4.1/32、目的 IP 地址为 192.168.2.2/32、目的端口号为 POP3 对
        应的著名端口号的 TCP 报文继续转发的过滤规则)
Router(config)#access-list 101 permit tcp host 192.1.4.1 host 192.168.2.2 eq smtp
        (允许源 IP 地址为 192.1.4.1/32、目的 IP 地址为 192.168.2.2/32、目的端口号为 SMTP 对
        应的著名端口号的 TCP 报文继续转发的过滤规则)
Router(config)#access-list 101 permit tcp host 192.1.3.2 host 192.168.2.2 eq smtp
        (允许源 IP 地址为 192.1.3.2/32、目的 IP 地址为 192.168.2.2/32、目的端口号为 SMTP 对
        应的著名端口号的 TCP 报文继续转发的过滤规则)
Router(config)#access-list 101 permit tcp host 192.1.3.2 eq smtp host 192.168.2.2
        (允许源 IP 地址为 192.1.3.2/32、源端口号为 SMTP 对应的著名端口号、目的 IP 地址为
        192.168.2.2/32 的 TCP 报文继续转发的过滤规则)
Router(config)#access-list 101 deny ip any any    (禁止一切 IP 分组继续转发的过滤规则)
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 101 out
                    (将编号为 101 的扩展过滤器作用于接口 FastEthernet0/1 输出方向)
Router(config-if)#exit
```

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.3.0
Router(config-router)#network 192.1.4.0
Router(config-router)#exit
```

(3) Router3 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.1 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.4.0
Router(config-router)#exit
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 1 deny any
Router(config)#ip nat inside source list 1 interface FastEthernet1/0 overload
Router(config)#ip nat inside source static tcp 192.168.2.1 80 192.1.4.1 80
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.1
Router(config)#access-list 101 permit tcp host 192.1.2.1 host 192.168.2.1 eq www
Router(config)#access-list 101 deny ip any any
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 101 out
Router(config-if)#exit
```

6.3.4 路由器身份鉴别实验

1. 实验内容

(1) 完成网络设计和配置。

(2) 完成路由器 PPP 配置。

(3) 配置路由器 PPP 身份鉴别机制。

(4) 验证网络之间的连通性。

2. 网络结构

网络结构如图 6.44 所示。路由器 R1 和 R2 通过串行链路互连，如果采用 PPP 作为串行链路的链路层协议，为了实现两个路由器之间的通信过程，首先需要建立两个路由器之间的 PPP 链路，一旦 PPP 启动身份鉴别机制，只有在双方相互完成身份鉴别后，才能成功建立 PPP 链路。

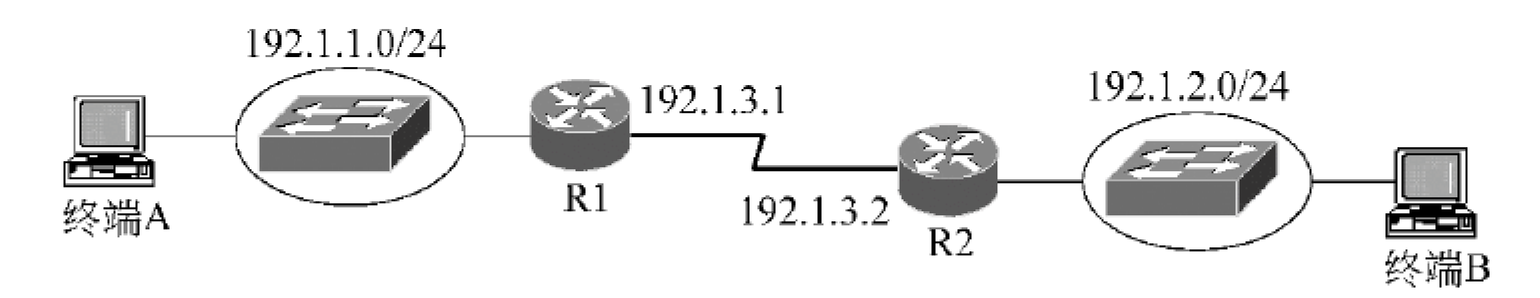


图 6.44　实现路由器身份验证网络结构

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 6.44 所示的网络结构放置和连接设备，逻辑工作区完成设备放置和连接后的界面如图 6.45 所示。

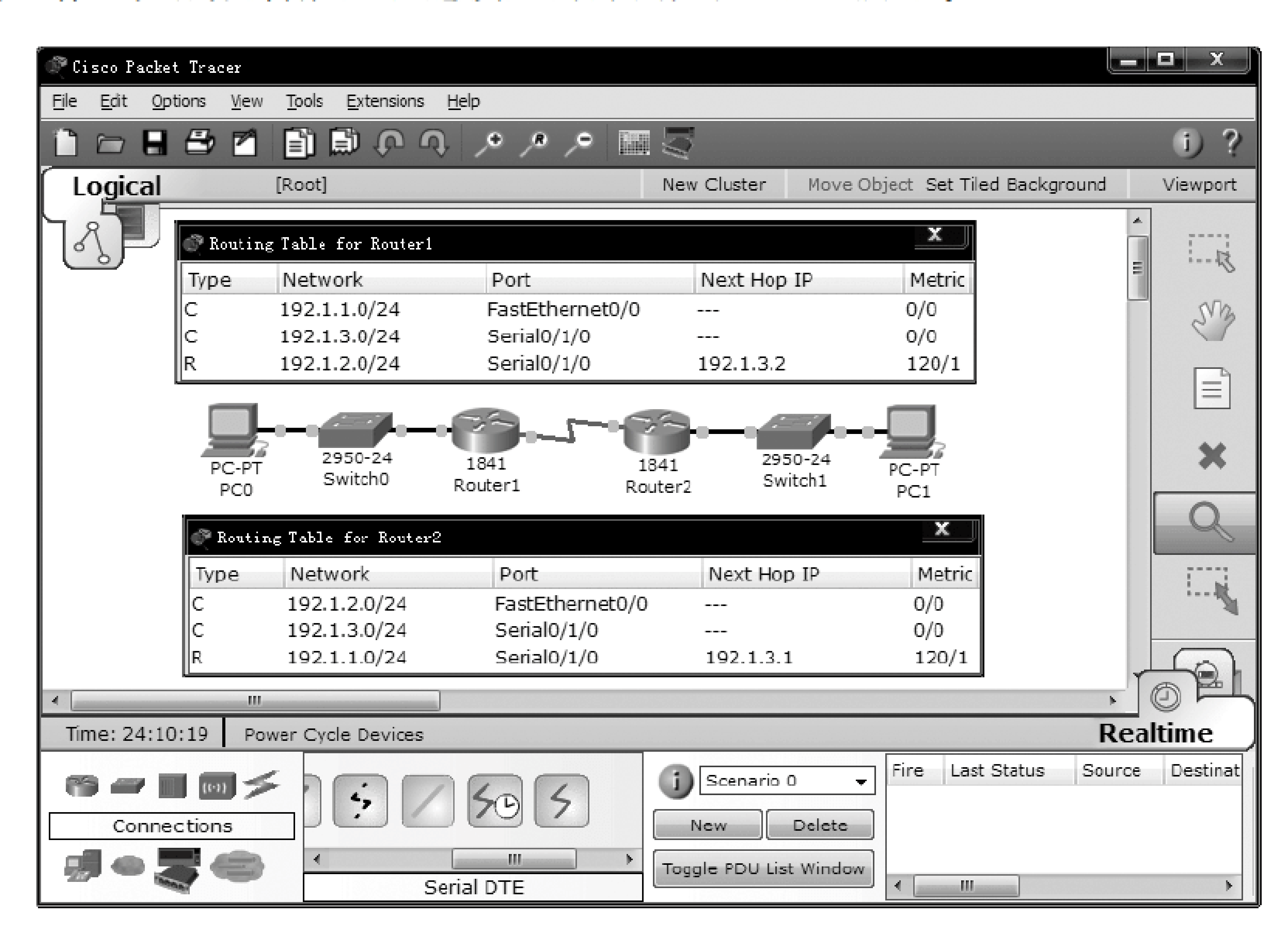


图 6.45　放置和连接设备后的逻辑工作区界面及路由表

(2) 根据图 6.44 所示配置信息完成路由器接口 IP 地址和子网掩码配置，完成路由器 RIP 配置，启动串行口，两个路由器生成图 6.45 所示的路由表。

(3) 路由器 Router1 通过命令 hostname r1 指定自己的主机名为 r1，通过命令 username r2 password 1234 指定相邻路由器主机名 r2 和鉴别相邻路由器身份使用的密码 1234。在串行口配置模式通过命令“encapsulation ppp”指定链路层协议 PPP，通过命令“ppp authentication chap”指定用鉴别协议 chap 鉴别相邻路由器身份。完成上述操作

后，查看两个路由器中的路由表，发现只剩下一项目的网络为以太网端口直接连接的网络的路由项。

（4）路由器 Router2 通过命令 hostname r2 指定自己的主机名为 r2，通过命令 username r1 password 1234 指定相邻路由器主机名 r1 和鉴别相邻路由器身份使用的密码 1234，对串行口完成 Router1 相同的配置。此时，两个路由器重新生成图 6.45 所示的路由表，表示成功建立互连两个路由器的 PPP 链路，而成功建立 PPP 链路的前提是两个路由器各自完成对相邻路由器的身份鉴别。

4. 命令行配置过程

（1）Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface Serial0/1/0          (进入串行接口配置模式)
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.1 255.255.255.0
Router(config-if)#clock rate 4000000          (指定串行接口数据传输速率)
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.1.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#hostname r1                    (指定路由器主机名为 r1)
r1(config)#username r2 password 1234
                    (指定相邻路由器主机名 r2 和用于鉴别相邻路由器身份时使用的密码 1234)
r1(config)#interface Serial0/1/0
r1(config-if)#encapsulation ppp          (指定串行接口的链路层协议为 PPP)
r1(config-if)#ppp authentication chap    (指定 PPP 用鉴别机制 chap 鉴别相邻路由器身份)
r1(config-if)#exit
```

（2）Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#no shutdown
Router(config-if)#clock rate 4000000
```

```
Router(config-if)#ip address 192.1.3.2 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#hostname r2
r2(config)#username r1 password 1234                (双方必须配置相同的密码 1234)
r2(config)#interface Serial0/1/0
r2(config-if)#encapsulation ppp
r2(config-if)#ppp authentication chap
r2(config-if)#exit
```

第7章 无线局域网安全技术

CHAPTER

7.1 知识要点

7.1.1 WEP

1. 加密机制

(1) 采用流密码体制

$Y= P \oplus K_i$(其中 Y 是密文,P 是明文,K_i 是一次性密钥),一次性密钥通过单向函数 FR(K,**IV**)产生,K 是密钥,在计算一次性密钥时作为常量,**IV**(Initialization Vector,初始向量)是 24 位长度的变量,单向函数 FR 保证,当 **IV** 变化时,FR(K,**IV**)也随之发生变化,因此对应 **IV** 的 2^{24}种不同组合,存在一次性密钥集$\{K_0,K_1,\cdots,K_{i-1}\}$,$i=2^{24}$。

(2) 同一基本服务集中终端具有相同的密钥 K

所有需要和相同的 AP 建立关联的终端分配同一个密钥 K,802.11 没有限定终端选择 **IV** 的方式,如果两个终端选择相同的 **IV**,则产生部分相同(两个一次性密钥长度不同的情况),或完全相同(两个一次性密钥长度相同的情况)的一次性密钥,因此不同的终端可能采用相同的一次性密钥加密数据。同一基本服务集中的所有终端共享一个由 2^{24}个不同一次性密钥构成的一次性密钥集。

2. 鉴别机制

WEP 鉴别过程就是判断终端是否是授权终端的过程,判断某个终端是否授权的依据是该终端是否拥有和 AP 相同的密钥 K。如图 7.1 所示。鉴别过程由终端发起,首先由终端向 AP 发送鉴别请求,AP 向终端发送固定长度的随机数 challenge,终端选择 **IV**,并计算出 $Y=\text{challenge} \oplus \text{FR}(K,\textbf{IV})$,将密文 Y 和 **IV** 一起发送给 AP,AP 根据自己的密钥 K'和终端发送的 IV 计算出 $P=Y \oplus \text{FR}(K',\textbf{IV})$,如果 $\text{P}= \text{challenge}$,表示 $K=K'$,判断终端是授权终端。否则,判断终端不是授权终端。

3. WEP 的缺陷

WEP 的缺陷主要有三项:一是所有终端共享同一个密钥 K,容易导致

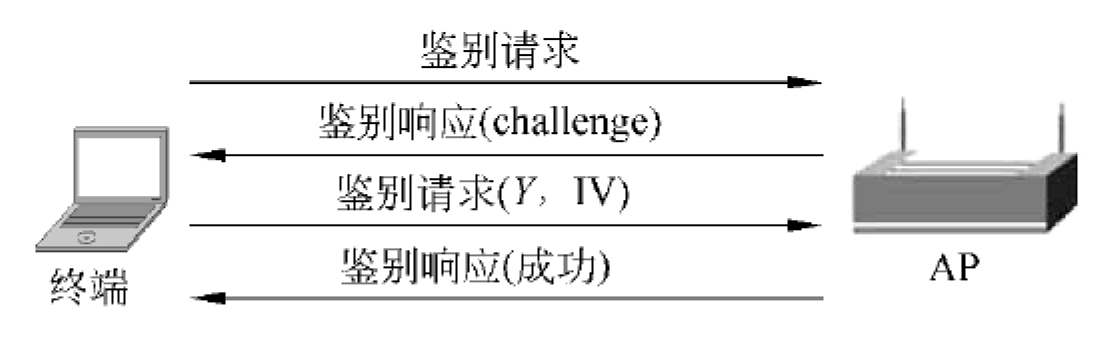


图 7.1　WEP 鉴别过程

密钥外泄。二是所有终端共享由 2^{24} 个不同一次性密钥构成的一次性密钥集，使得黑客可以通过建立一次性密钥字典来破译密文。三是鉴别机制存在较大漏洞，容易被黑客破解。

7.1.2　WPA

WPA(Wi-Fi Protected Access，Wi-Fi 保护访问)是一种和 802.11i 兼容的安全协议，WPA 兼容 2003 年颁布的 802.11i 草稿，WPA2 兼容 2004 年颁布的 802.11i 标准。Wi-Fi 联盟主要提供 WLAN 产品的兼容性认证。

1. 鉴别机制

WPA 基于用户身份进行身份鉴别，标识用户身份的信息有用户名和口令、认证中心颁发的证书和私钥等。这种身份鉴别过程通常需要配置鉴别服务器，如图 7.2 所示，AP 作为 NAS 用于向鉴别服务器转发用户鉴别信息。图 7.3 给出用户标识信息为用户名和口令时的用户身份鉴别过程。完成身份鉴别后，由终端和鉴别服务器根据用户标识信息产生成对主密钥(Pairwise Master Key，PMK)，并由鉴别服务器以加密方式将 PMK 传输给 AP。

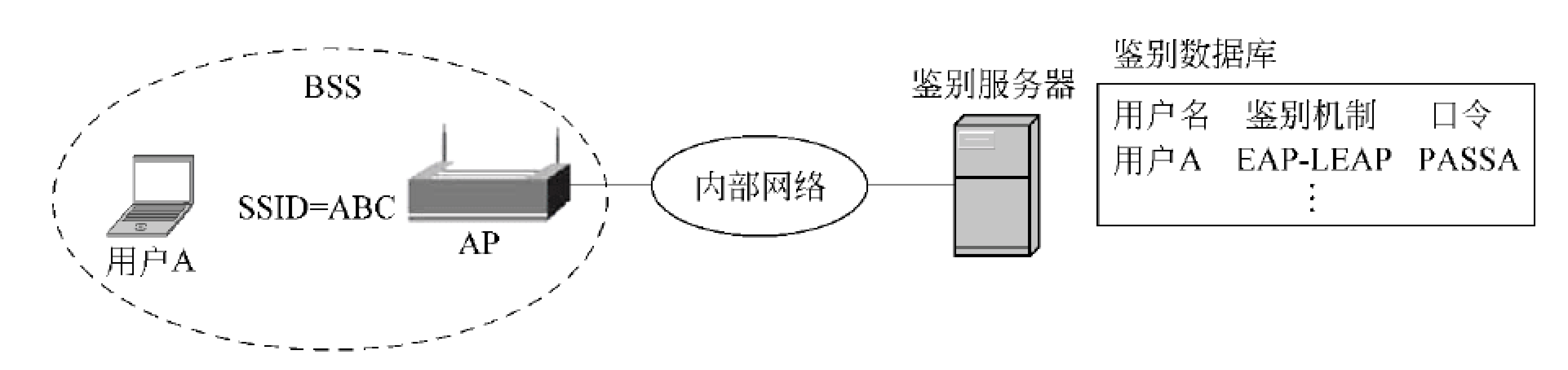


图 7.2　实现 WPA 鉴别过程的网络结构

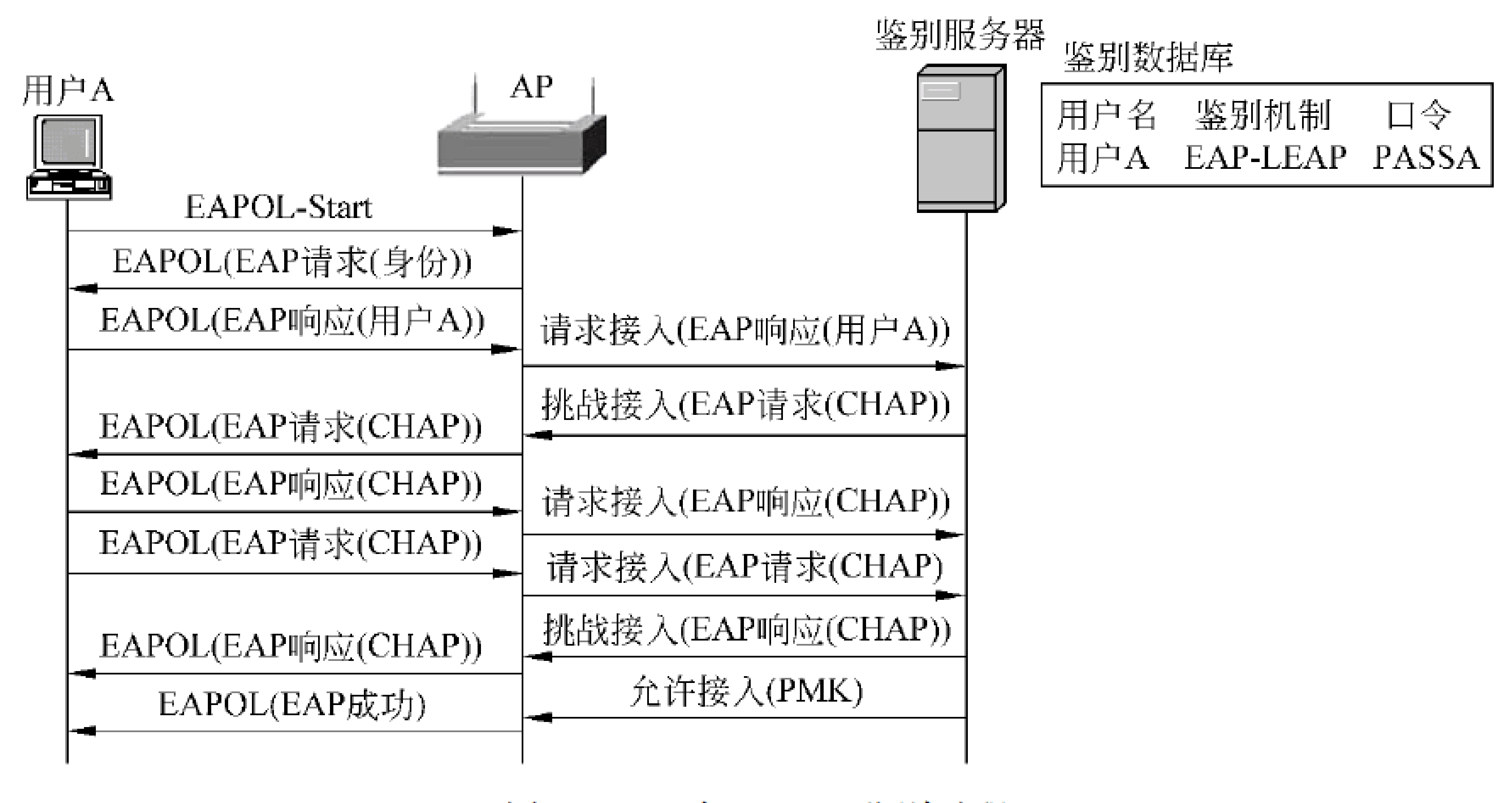


图 7.3　双向 CHAP 鉴别过程

WPA 实施密钥分配的前提是终端和 AP 拥有相同的 PMK，但通过 PMK 产生密钥过程中：一是需要使用双方随机选择的随机数 AN(AP 选择的随机数)和 SN(终端选择的随机数)，这就保证，对于同一 PMK，每一次密钥分配过程产生的密钥都是不同的；二是产生密钥过程中，需要使用终端和 AP 的 MAC 地址，这就保证，对于不同终端，产生的密钥是不同的。图 7.4 所示是密钥分配过程，整个过程实现三项功能：一是交换各自产生的随机数 AN 和 SN；二是根据图 7.5 所示计算过程产生密钥；三是证实终端和 AP 拥有相同的 PMK。

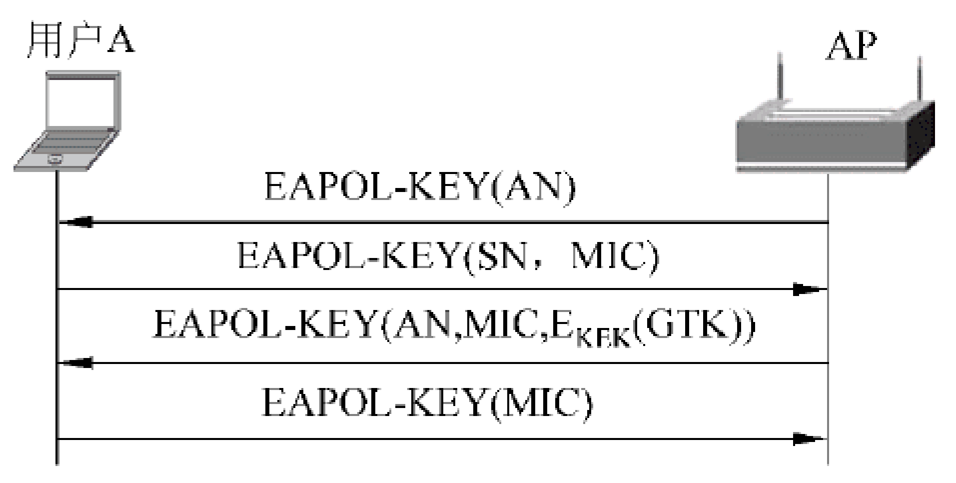


图 7.4　密钥分配过程

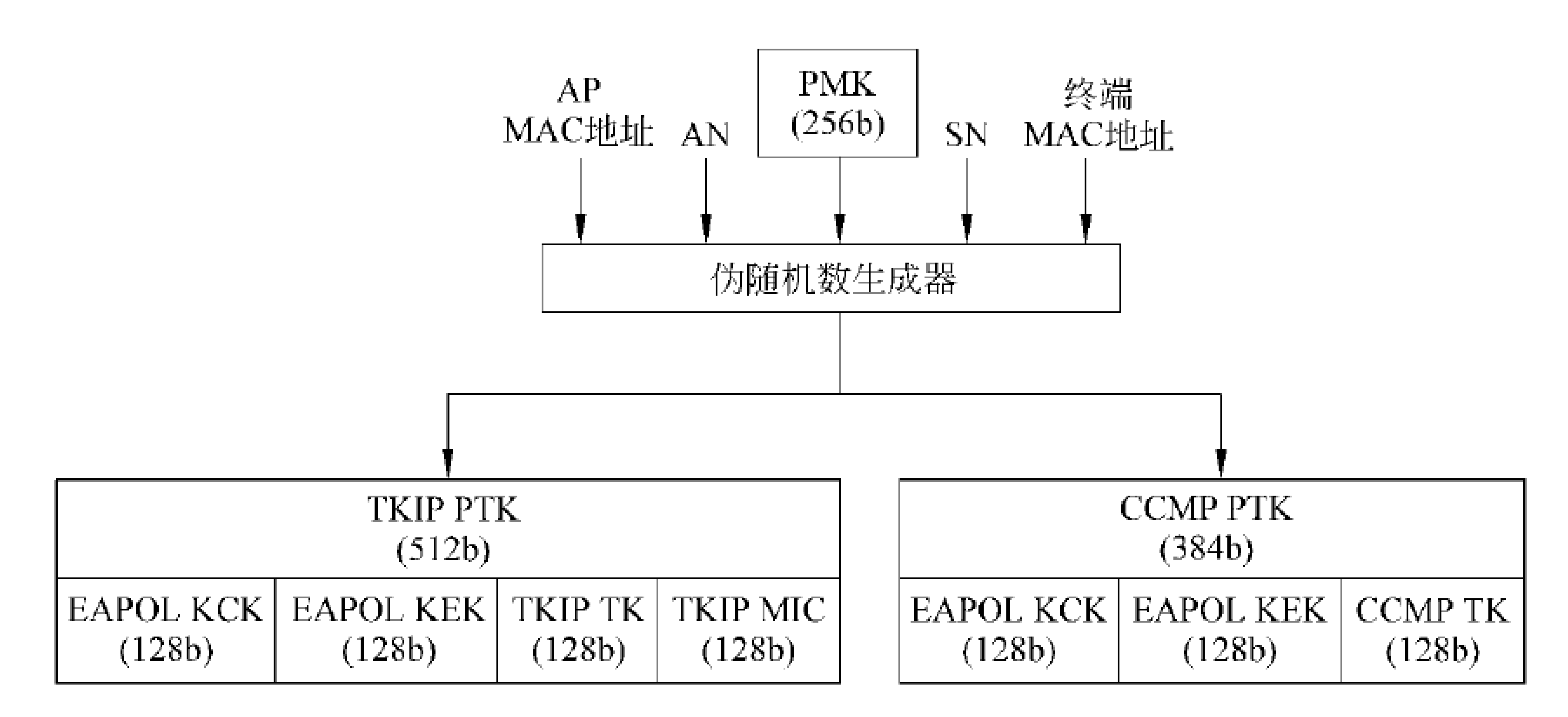


图 7.5　密钥计算过程及结构

2. 加密机制

WPA 本质上仍然采用流密码体制，只是一次性密钥集的产生过程与 WEP 不同。

对于临时密钥完整性协议(Temporal Key Integrity Protocol，TKIP)，产生一次性密钥的单向函数的参数是 TK 和 TSC(FR(TK，TSC))。一是和 WEP 不同，每一个终端和 AP 之间有着单独的 TK，而且对于同一个终端，每一次密钥分配过程产生的 TK 也是不同的。二是 TSC 的长度为 48 位，在 TK 不变的前提下，可以有 2^{48} 个不同的一次性密钥。

对于 CCMP(CTR with CBC-MAC Protocol)，除了单向函数的参数变为和 TKIP 中 TK 和 TSC 相同含义的 TK 和 PN 外，单向函数 FR 由对称密钥加密算法 AES 实现。显然，AES 比 WEP 和 TKIP 采用的单向函数有着更好的单向性和安全性。

3. WPA-PSK

WPA-PSK 和 WPA 的不同在于省略了基于用户标识信息的身份鉴别过程和 PMK 动态生成过程，而是在 AP 和所有需要和该 AP 建立关联的终端上静态配置相同的 PMK。鉴别过程就是判断某个终端是否拥有和 AP 相同的 PMK 的过程，因此，图 7.4 所示的密钥分配过程也是终端的鉴别过程，因为密钥分配过程成功进行的前提是终端和 AP 拥有相同的 PMK。和 WEP 不同的是，不同终端分配到的 TK 不同，同一终端每一次

密钥分配过程分配到的 TK 也不同。

7.2 例题解析

7.2.1 自测题

1. 选择题

(1) 无线局域网最大的问题是________。

A. 可靠性低　B. 安全性差　C. 传输速率低　D. 移动通信能力弱

(2) 无线局域网开放性带来的安全问题是________。

A. 黑客能够轻易接入　B. 黑客能够轻易嗅探数据

C. 传播的信号易受干扰　D. A 和 B

(3) 关于 WEP,下述________描述是错误的。

A. 用循环冗余码检测数据完整性

B. 伪随机数生成算法作为产生一次性密钥的单向函数

C. 采用流密码体制

D. 一次性密钥不会重复

(4) 关于 WEP 鉴别过程,下述________描述是错误的。

A. 授权终端必须具有和 AP 相同的密钥 K

B. AP 发送固定长度的随机数 P

C. 终端发送 $P \oplus \mathrm{FR}(K,\mathbf{IV})$ 和 **IV**

D. 黑客无法得到 $\mathrm{FR}(K,\mathbf{IV})$ 和 **IV**

(5) 关于 WEP 加密,下述________描述是错误的。

A. 终端和 AP 必须具有相同密钥 K

B. 为了同步一次性密钥,发送端需要向接收端发送 **IV** 明文

C. 黑客无法通过嗅探经过无线网络传输的信息获得密钥 K

D. 黑客无法破译嗅探到的经过无线网络传输的密文

(6) 下述________不属于 WEP 的缺陷。

A. 所有终端配置相同的密钥

B. 在密钥不变的情况下,只有 2^{24} 个一次性密钥

C. 循环冗余码用于完整性检测

D. 使用流密码体制

(7) 下述________不是 WPA 优于 WEP 的地方。

A. 基于用户接入控制

B. 基于用户生成密钥

C. 每一个用户单独拥有 2^{48} 个一次性密钥

D. 使用流密码体制

(8) 下述________不是 WPA-PSK 优于 WEP 的地方。

A. 所有终端配置相同的密钥
B. 采用更好的完整性检测算法
C. 每一个终端单独拥有 2^{48} 个一次性密钥
D. 鉴别过程更加安全

(9) 下述________描述是错误的。
A. WEP 在密钥有效期间，所有终端共享 2^{24} 个一次性密钥
B. WPA-PSK 在密钥有效期间，每一个终端单独拥有 2^{48} 个一次性密钥
C. WPA-PSK 根据是否拥有和 AP 相同的 PMK 判断是否是授权终端
D. WPA 在安全关联存在期间，每一个用户单独拥有 2^{48} 个一次性密钥

(10) 下述________描述是正确的。
A. 获取 WEP 密钥能够破译一切经过无线局域网传输的密文
B. 获取 WPA-PSK 密钥能够破译一切经过无线局域网传输的密文
C. 获取 WPA 用户标识信息能够破译一切经过无线局域网传输的密文
D. 一旦和 AP 成功建立关联，便能够破译一切经过无线局域网传输的密文

(11) 关于 TKIP，下述________描述是错误的。
A. 仍然是流密码体制
B. 采用 Michael 算法计算消息鉴别码
C. 在 TK 不变的情况下，每一个终端拥有 2^{48} 个一次性密钥
D. 如果一些终端的 TK 相同，这些终端共享 2^{48} 个一次性密钥

(12) 关于 CCMP，下述________描述是错误的。
A. 消息鉴别码计算过程中包含 MAC 帧首部中传输过程中不变的字段
B. 消息鉴别码计算过程中使用 AES 加密算法和分组加密链接模式
C. 一次性密钥计算过程中使用 AES 加密算法和计数器模式
D. 使用 AES 加密算法和分组加密链接模式加密分组后的数据

(13) 关于 WPA 和 WPA-PSK，下述________描述是错误的。
A. WPA 针对每一个用户动态产生 PMK，WPA-PSK 静态配置 PMK
B. WPA 和 WPA-PSK 对每一个终端产生不同的 TK
C. WPA 下，黑客获得某个用户的标识信息可以成功接入无线局域网
D. WPA-PSK 下，黑客获得 PMK 可以破译经过无线局域网传输的所有密文

2. 填空题

(1) WEP 一次性密钥集共有________个一次性密钥，所有终端共享________个一次性密钥，黑客获得密钥，能够________。

(2) WPA 下，每一个用户具有不同的________，针对每一个用户动态产生________，每一次建立安全关联，产生不同的________。

(3) WPA-PSK 下，所有和同一 AP 建立关联的终端静态配置________，每一个终端每一次密钥分配过程产生不同的________。

(4) 如果一些终端有着相同的 TK，这些终端________。

(5) WPA 下，鉴别过程要求证明用户具有________。WPA-PSK 下，鉴别过程要求

终端证明具有________。无论是WPA,还是WPA-PSK,鉴别过程均可实现________。

(6) WPA下,如果某个授权用户的用户标识信息外泄,需要________。WPA-PSK下,如果PMK外泄,需要________。WEP下,如果密钥外泄,需要________。

(7) WPA和WPA-PSK在网络结构上的最大不同在于WPA需要________。WPA下,用户可以接入任何的BSS。WPA-PSK下,终端可以接入________。

(8) TKIP用________产生消息鉴别码,用________产生一次性密钥,计算消息鉴别码过程中包含________。CCMP用________产生消息鉴别码,用________产生一次性密钥,计算消息鉴别码过程中包含________。

(9) 802.1X密钥分配过程中,通过________和________保证同一终端每一次密钥分配过程产生不同的TK,通过________保证不同终端产生不同的TK。

(10) TK是________,只用于实现________和________之间数据加密传输。

3. 名词解释

____ MAC	____ MIC
____ WEP	____ TKIP
____ CCMP	____ TK
____ WPA	____ WPA-PSK
____ 802.11i	____ Michael
____一次性密钥	____密钥
____ BSS	____ ESS
____ CRC	____ AP
____ KEK	____ GTK
____ PN	____ ICV
____ PMK	____ SSID
____ IV	____ TSC
____ PTK	____ KCK

(a) 有线等效保密,802.11定义的一种安全机制,其目的是使无线局域网具有以太网的安全性。

(b) 临时密钥完整性协议,WPA定义的一种用于数据加密和完整性检测的协议,其安全性好于WEP提供的数据加密和完整性检测机制。

(c) WPA定义的一种用于数据加密和完整性检测的协议,通过AES对称密钥加密算法和加密分组链接模式计算消息鉴别码,通过AES对称密钥加密算法和计数器模式计算一次性密钥。

(d) 临时密钥,在TKIP和CCMP中用于计算一次性密钥。在WPA和WPA-PSK中,TK往往是成对临时密钥,即每一个终端和AP拥有独立的TK。

(e) Wi-Fi保护访问,Wi-Fi联盟定义的一种和802.11i兼容的安全协议,用TKIP和CCMP实现数据加密和完整性检测,用802.1X和EAP实现身份鉴别。

(f) 一种通过配置和AP相同的PMK完成鉴别过程,其他和WPA相同的安全协议。

(g) 一种由IEEE指定的标准,其内容与WPA相同。

(h) TKIP 用于计算消息鉴别码的一种算法。

(i) 消息鉴别码,用于接收端检测消息的完整性。

(j) 消息完整性编码,其作用等同于 MAC。

(k) 循环冗余码,本是一种检错码,WEP 却用于实现数据完整性检测。

(l) 接入点,一种用于实现无线局域网和分配系统互连的设备。

(m) 基本服务集,一个由移动终端和 AP 构成的无线局域网最小单位。

(n) 扩展服务集,一个由分配系统互连在一起的多个 BSS 组成的无线局域网单位。

(o) 初始向量,一个 24 位二进制数,WEP 中和密钥一起构成随机数种子,用于产生作为一次性密钥的随机数。

(p) TKIP 序号计数器,一个 48 位二进制数,TKIP 中和 TK、发送端 MAC 地址一起构成随机数种子,用于产生作为一次性密钥的随机数。

(q) 报文编号,一个 48 位二进制数,CCMP 用于产生一次性密钥和防止重放攻击。

(r) 完整性检验值,WEP 用于实现数据完整性检测的循环冗余码。

(s) 流密码体制中用于每一次加密数据的密钥,需要保证:一是不重复,每一次加密数据的密钥不同;二是密钥之间没有关联性,即无法通过以前加密数据的密钥预测这一次和以后加密数据的密钥。

(t) 作为计算一次性密钥的函数的其中一个参数,用于在多个一次性密钥集中选择一个一次性密钥集。某个终端是否拥有该参数常被用来作为判断该终端是否是授权终端的依据。

(u) 成对主密钥,WPA 下,完成身份鉴别过程后自动产生,每一个用户和 AP 之间独立产生成对主密钥。WPA-PMK 下,在所有终端和 AP 静态配置成对主密钥。

(v) 服务集标识符,用于唯一标识某个基本服务集,属于该基本服务集的终端和 AP 需配置相同的服务集标识符。

(w) 成对过渡密钥,以 PMK、AP 和终端 MAC 地址、AP 和终端生成的随机数为参数计算出的足够位数的密钥,可以通过分解该密钥产生完成数据加密和完整性检测所需的其他密钥,如 TK。

(x) 证实密钥,用于证实终端和 AP 计算出相同的 PTK。由于终端和 AP 计算出相同的 PTK 的前提是终端和 AP 具有相同的 PMK,因此证实密钥用于证实终端和 AP 具有相同的 PMK。

(y) 加密密钥,用于 AP 加密传输给终端的临时广播密钥。

(z) 临时广播密钥,用于 AP 加密在 BSS 中广播的数据。

4. 判断题

(1) WEP 鉴别机制容易导致黑客通过 AP 对其的身份鉴别。

(2) WEP 鉴别过程是单向鉴别,只能由 AP 鉴别终端身份。

(3) 黑客容易通过嗅探经过无线局域网传输的密文破译密钥。

(4) WEP 容易通过同时改变净荷密文和 ICV 密文,使得接收端检测不出已经发生的篡改。

(5) WEP 和 WPA-PSK 要求所有终端和 AP 配置相同的密钥。

(6) WPA 在完成对用户的身份鉴别过程中动态产生 PMK，且每一个用户和 AP 有着独立的 PMK。

(7) WPA 下，某个授权用户的用户标识信息泄漏需要在鉴别服务器中删除或修改该用户标识信息。

(8) WEP 和 WPA-PSK 下，密钥泄漏需要修改 BSS 中所有终端和 AP 配置的密钥。

(9) WEP 下，获取密钥即可破译经过无线局域网传输的所有密文。

(10) WPA 下，获取某个授权用户的用户标识信息即可破译经过无线局域网传输的所有密文。

(11) WPA-PSK 下，获取 PMK 即可破译经过无线局域网传输的所有密文。

(12) TKIP 下，通过生成一次性密钥字典来破译密文是困难的。

(13) 每一个终端有着独立的 TSC 和 PN，且每发送一帧 MAC 帧，递增 TSC 和 PN，以此可以防止重放攻击。

(14) WPA-PSK 下，每一个终端和 AP 有着独立的 TK。

(15) 成功接入无线局域网表示可以和 AP，并经过 AP 和其他终端相互交换数据。

(16) 成功接入无线局域网表示可以破译经过无线局域网传输的所有密文。

(17) WPA-PSK 下，所有终端和 AP 静态配置相同的 PMK，但不同终端通过密钥分配过程中生成的 PTK 是不同的。

7.2.2 自测题答案

1. 选择题答案

(1) B，开放性导致无线局域网的安全性差。

(2) D，任何能够进入无线电信号传播范围，且具有指定信道数据接收能力的终端，都可嗅探经过无线局域网传输的数据。

(3) D，所有终端共享 2^{24} 个一次性密钥很容易导致一次性密钥重复使用。

(4) D，如果黑客嗅探到 P、$P \oplus \text{FR}(K,\mathbf{IV})$ 和 **IV**，很容易通过 $\text{P} \oplus \text{P} \oplus \text{FR}(K,\mathbf{IV}) = \text{FR}(K,\mathbf{IV})$ 得到 $\text{FR}(K,\mathbf{IV})$ 和 **IV**。

(5) D，一旦黑客建立一次性密钥字典，黑客通过 **IV** 检索出对应的一次性密钥，并用该一次性密钥破译密文。

(6) D，流密码体制本身没有安全缺陷。

(7) D，差别不是流密码体制，而是一次性密钥生成过程。

(8) A，WPA-PSK 同样要求 BSS 中的所有终端和 AP 静态配置相同的 PMK。

(9) B，WPA-PSK 下，同一终端每一次密钥分配过程产生不同的 TK，每个终端对应每一个 TK 有着 2^{48} 个一次性密钥，在 PMK 有效期间，可以有无数次的密钥分配过程。

(10) A，WEP 计算一次性密钥的参数是密钥 K 和初始向量 **IV**，初始向量 **IV** 以明文方式出现在 MAC 帧中，因此，一旦获得密钥 K，可以计算出对应任何初始向量的一次性密钥。其余三项只能实现和 AP 安全交换数据。

(11) D，TKIP 计算一次性密钥时，发送端 MAC 地址是其中一个参数，因此相同 TK，不同发送端 MAC 地址有着不同的一次性密钥集。

(12) D,仍然通过用计算出的一次性密钥和数据的异或操作完成数据加密。

(13) D,即使 PMK 相同,不同终端密钥分配过程生成的 TK 也不同,除非黑客嗅探到某个终端和 AP 之间密钥分配过程中相互交换的随机数 AN 和 SN,否则无法通过 PMK 推导出 TK,因而无法解密其他终端和 AP 交换的密文。

2. 填空题答案

(1) 2^{24},2^{24},破译所有经过无线局域网传输的密文。

(2) 用户标识信息,PMK,TK。

(3) 相同的 PMK,TK。

(4) 有着独立的 2^{48} 个一次性密钥。

(5) 和某个授权用户相同的用户标识信息,PMK,双向鉴别。

(6) 修改或删除该授权用户的用户标识信息,在同一 BSS 中的所有终端和 AP 配置新的 PMK,在同一 BSS 中的所有终端和 AP 配置新的密钥。

(7) 配置鉴别服务器,AP 的 PMK 和终端配置的 PMK 相同的 BSS。

(8) Michael 算法,伪随机数生成函数,源和目的终端地址,AES 和加密分组链接模式,AES 和计数器模式,MAC 帧首部中所有传输过程中不变的字段。

(9) AP 选择的随机数 AN,终端选择的随机数 SN,终端 MAC 地址。

(10) 成对临时密钥,AP,终端。

3. 名词解释答案

i	MAC	j	MIC
a	WEP	b	TKIP
c	CCMP	d	TK
e	WPA	f	WPA-PSK
g	802.11i	h	Michael
s	一次性密钥	t	密钥
m	BSS	n	ESS
k	CRC	l	AP
y	KEK	z	GTK
q	PN	r	ICV
u	PMK	v	SSID
o	IV	p	TSC
w	PTK	x	KCK

4. 判断题答案

(1) 对,黑客很容易嗅探到某个有效的一次性密钥和 IV 对,并因此通过 AP 的鉴别过程。

(2) 对,WEP 只对终端进行鉴别。

(3) 错,除非密钥外泄,否则获取密钥是困难的,但可以通过建立一次性密钥字典破译密文。

(4) 对,这是循环冗余码作为消息鉴别码的缺陷。

(5) 对,是否拥有和 AP 相同的密钥或 PMK 是判断终端是否是授权终端的依据。

(6) 对,WPA 根据用户鉴别信息动态生成 PMK,且该 PMK 只有该用户和 AP 知道。

(7) 对,只需修改或删除该用户标识信息,其他授权用户的用户标识信息不受影响,这是基于用户的身份鉴别机制的好处。

(8) 对,这是基于密钥的身份鉴别机制的坏处。

(9) 对,WEP 计算一次性密钥的参数是密钥 K 和初始向量 **IV**,初始向量 **IV** 以明文方式出现在 MAC 帧中,因此,一旦获得密钥 K,可以计算出对应任何初始向量的一次性密钥。

(10) 错,WPA 下,获取某个授权用户的用户标识信息可以和 AP 交换密文,但无法破译其他终端和 AP 交换的密文,因为每一个终端的 TK 都不同。

(11) 错,除非嗅探到某个终端密钥分配过程中交换的 AN 和 SN,否则无法通过 PMK 推导出其他终端的 TK。

(12) 对,每一次建立安全关联时产生不同的 TK,每一个 TK 对应 2^{48} 个一次性密钥。

(13) 对,TSC 和 PN 就是终端发送的 MAC 帧的序号。

(14) 对,计算 TK 时,终端 MAC 地址是输入参数之一。

(15) 对,终端和 AP 可以交换密文,其他接入终端和 AP 也可以交换密文,只是需要 AP 根据发送端地址解密密文,根据接收端地址重新计算密文。

(16) 错,每一个终端只能解密 AP 发送给它的密文。

(17) 对,计算 PTK 时,终端 MAC 地址是输入参数之一。

7.2.3 简答题解析

1. 简述 WEP 的缺陷。

回答:一是由于密钥有效期间,所有终端共享 2^{24} 个一次性密钥,因此很容易通过建立一次性密钥字典破译密文。二是一旦黑客获得密钥,即可破译经过无线局域网传输的所有密文。三是身份鉴别机制容易被黑客破解。四是完整性检测机制无法检测出精心设计的篡改。

2. 简述 WEP、WPA 和 WPA-PSK 的差异。

回答:WEP 为所有终端和 AP 静态配置相同的密钥,根据是否拥有和 AP 相同的密钥作为判断该终端是否是授权终端的依据,用伪随机数生成函数产生一次性密钥,24 位初始向量和密钥作为随机数种子,所有终端密钥有效期间共享 2^{24} 个一次性密钥。用循环冗余码作为消息鉴别码。

WPA 为每一个授权用户单独配置用户标识信息,是否能够提供和某个授权用户相同的用户标识信息作为判断该用户是否是授权用户的依据,每一个用户身份鉴别过程中生成独立的 PMK,每一次密钥分配过程生成不同的 TK,每一个终端对应每一个 TK 有着 2^{48} 个一次性密钥,由于 TK 只有终端和 AP 知道,每一个终端只能解密 AP 发送给它的密文。使用比 WEP 安全性更高的一次性密钥生成算法和消息鉴别码生成算法。

WPA-PSK 和 WPA 不同的是省略了基于用户的身份鉴别过程和 PMK 动态生成过程。为所有终端和 AP 静态配置相同的 PMK,根据是否拥有和 AP 相同的 PMK 作为判

断该终端是否是授权终端的依据。由于 TK 计算过程中终端 MAC 地址、AP 和终端选择的随机数都作为输入参数，除非嗅探到密钥分配过程中 AP 和终端交换的两个随机数，否则某个终端无法通过 PMK 推导出另一个终端的 TK。但存在某个终端通过嗅探到另一个终端和 AP 在密钥分配过程中交换的两个随机数，从而推导出另一个终端的 TK 的可能性是 WPA-PSK 的最大安全隐患。和 WPA 不同用户动态生成不同的 PMK 相比，WPA-PSK 的安全性要弱得多。

3. 简述 TKIP 和 CCMP 的差异。

回答：一是计算消息鉴别码的算法，TKIP 采用 Michael 算法，CCMP 采用 AES 和加密分组链接模式。二是计算消息鉴别码时，TKIP 除了净荷外，只包括源和目的终端地址，CCMP 包含 MAC 帧首部中所有传输过程中不变的字段。三是一次性密钥计算方法，TKIP 采用伪随机数生成函数，CCMP 采用 AES 和计数器模式。四是 TKIP 使用不同的密钥计算消息鉴别码和一次性密钥，CCMP 用同一个密钥计算消息鉴别码和一次性密钥。

7.3　实　　验

7.3.1　WPA-PSK 配置实验

1. 实验内容

(1) 完成无线局域网和以太网互连。

(2) 完成终端和 AP 的 WPA-PSK 配置。

(3) 验证移动终端访问网络资源过程。

2. 网路结构

终端 A、B、C 和 AP 构成一个基本服务集，在建立终端和 AP 之间的关联后，终端通过 DHCP 自动配置过程获取网络配置信息。终端获取网络配置信息后，可以成功访问 Web 服务器。终端和 AP 采用 WPA-PSK 安全协议，因此需要在所有终端和 AP 上静态配置相同的 PMK，PMK 要求是 8～63 个 ASCII 字符，由终端和 AP 将其转换成 256 位的二进制数。

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 7.6 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 7.7 所示。

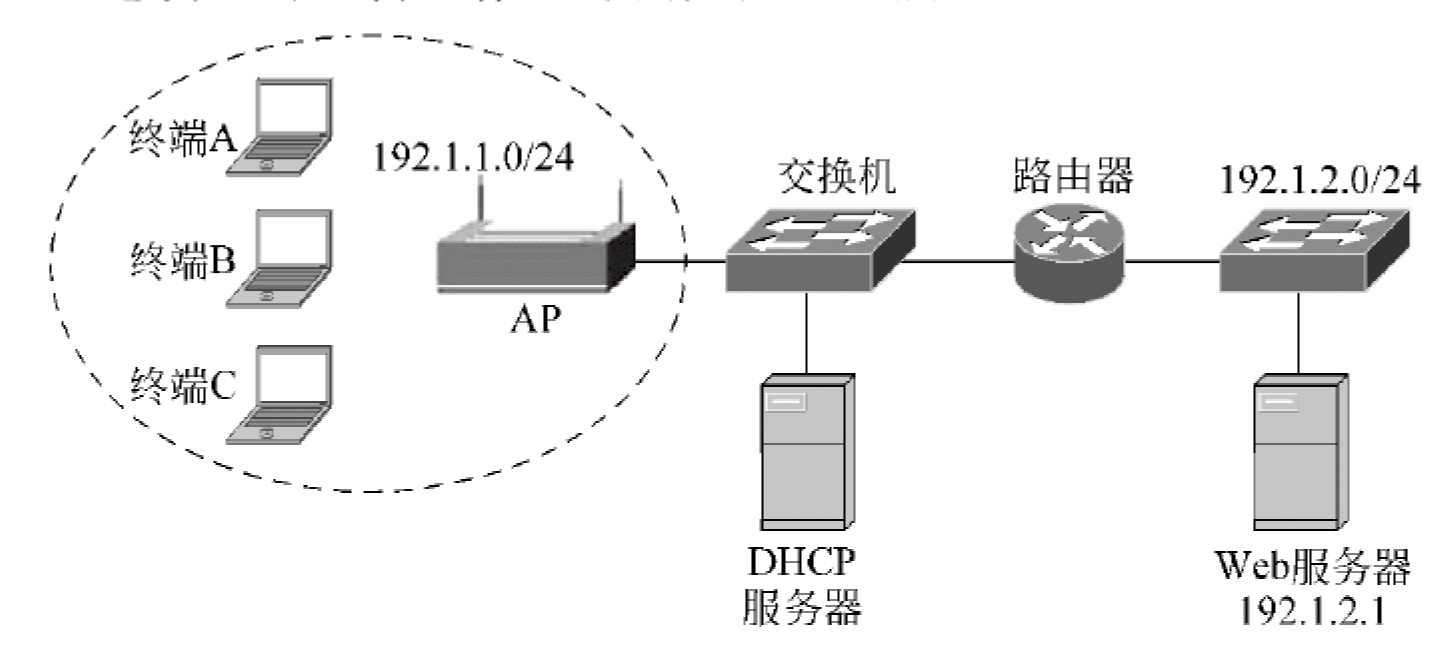


图 7.6　WPA-PSK 配置网络结构

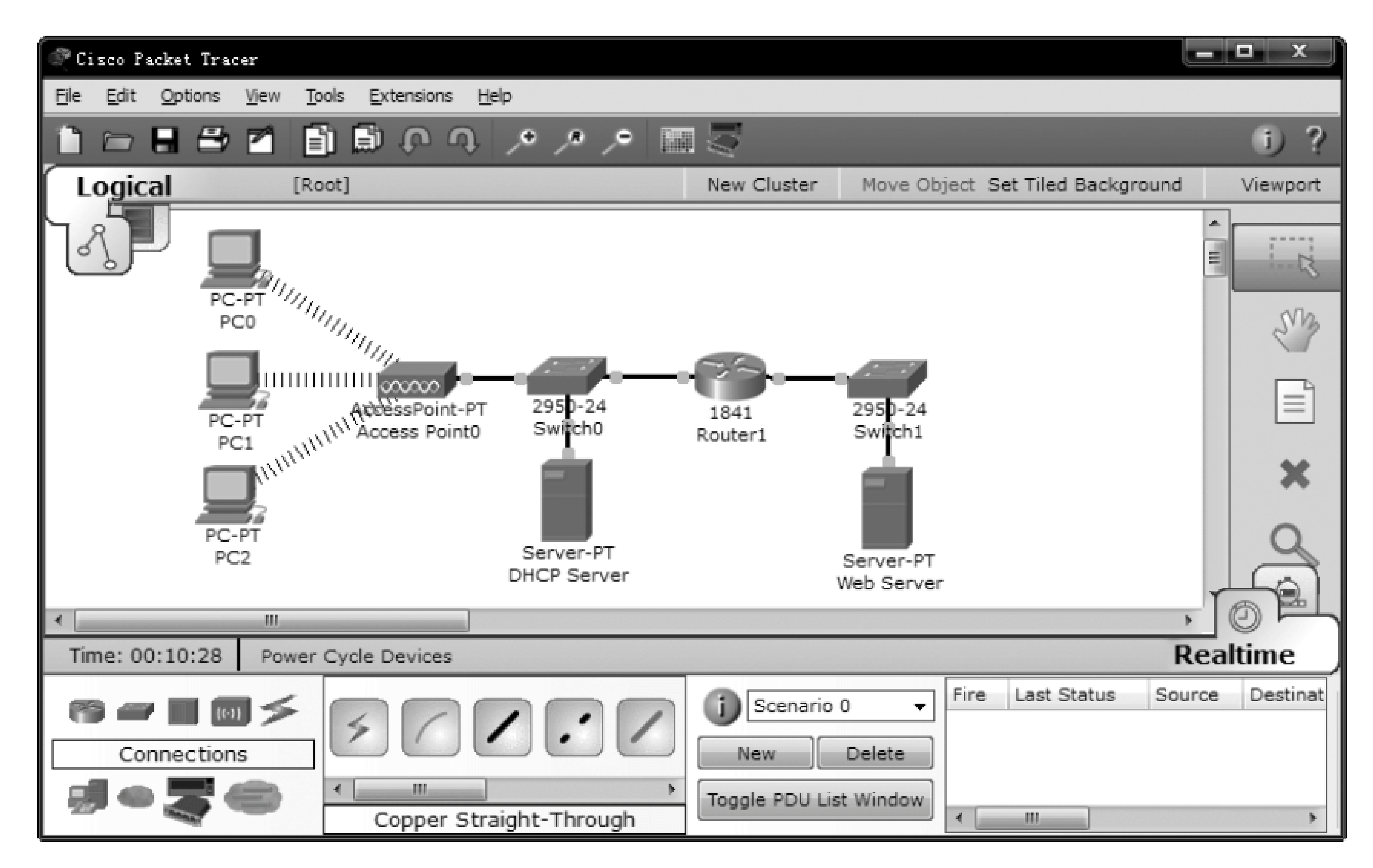


图 7.7 放置和连接设备后的逻辑工作区界面

(2) 开始终端和 AP 的 WPA2-PSK 配置。进入 AP 无线端口(port 1)配置界面,选中 WPA2-PSK 单选按钮,在 PassPhrase 文本框中输入 ASCII 字符 12345678,如图 7.8 所示。同样,进入终端 PC0 无线接口(Wireless)配置界面,选中 WPA2-PSK 单选按钮,在 PassPhrase 文本框中输入 ASCII 字符 12345678,如图 7.9 所示。在终端 PC1 和 PC2 中完成和 PC0 相同的配置。完成终端和 AP 的 WPA2-PSK 配置后,终端和 AP 之间成功建立关联,图 7.7 是终端和 AP 之间成功建立关联后的示意图。

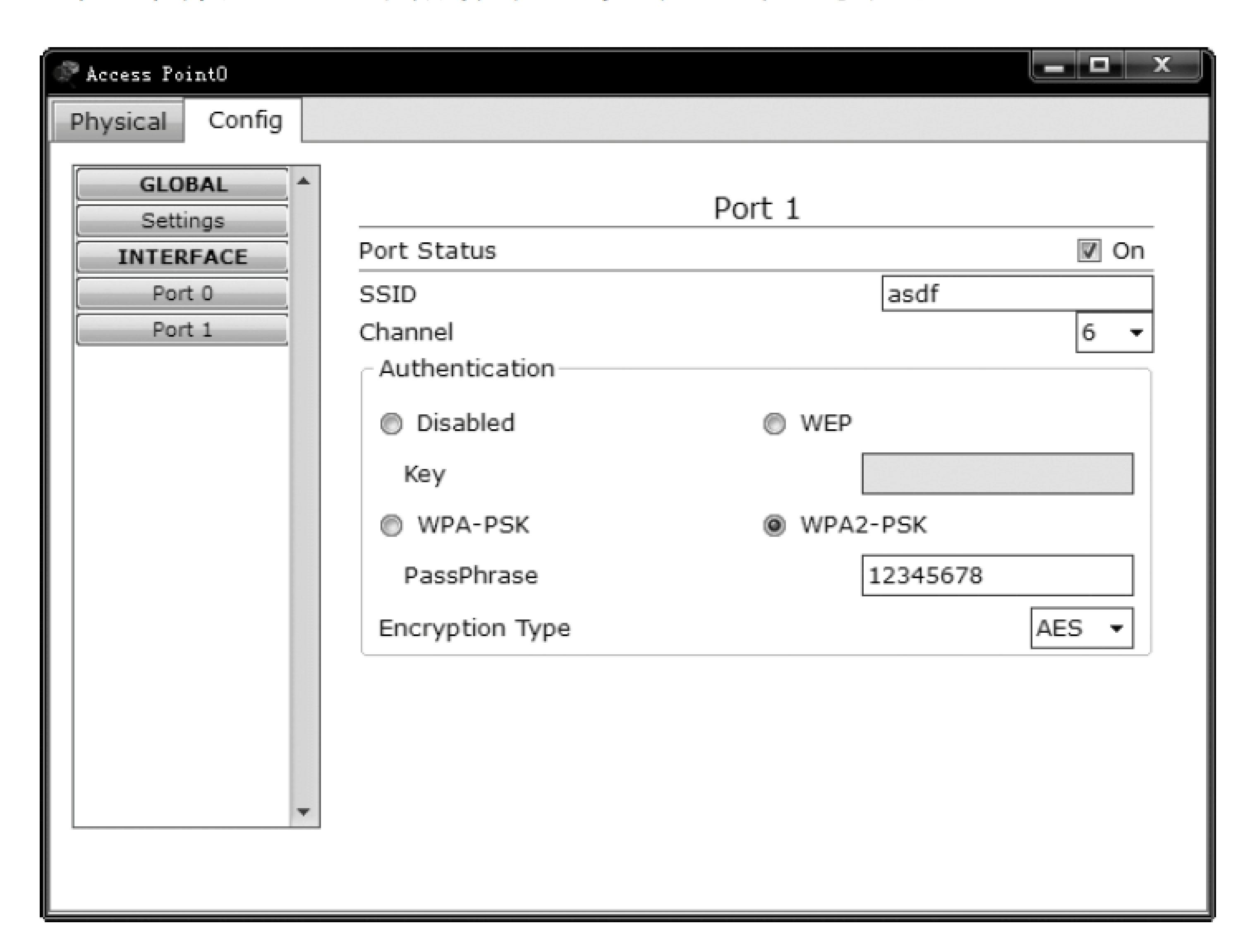


图 7.8 AP WPA2-PSK 配置界面

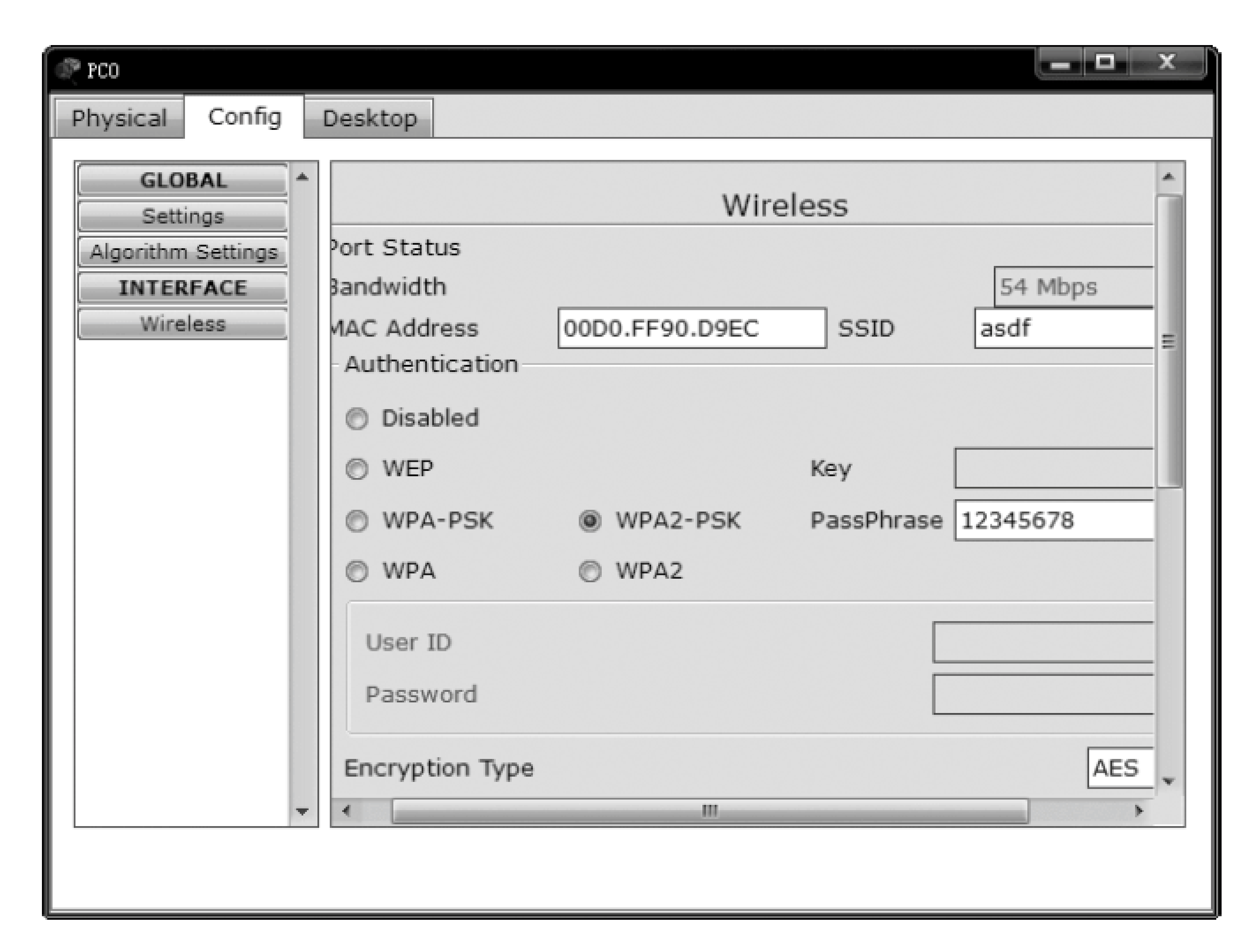


图 7.9　PC0 WPA2-PSK 配置界面

(3) 在 DHCP 服务器中为终端配置 IP 地址池，图 7.10 是 DHCP 服务器配置地址池的界面，这里为终端设置的默认网关地址为 192.1.1.254，IP 地址范围为 192.1.1.7～192.1.1.36。图 7.11 所示是 PC0 通过 DHCP 自动配置过程获取的网络配置信息。

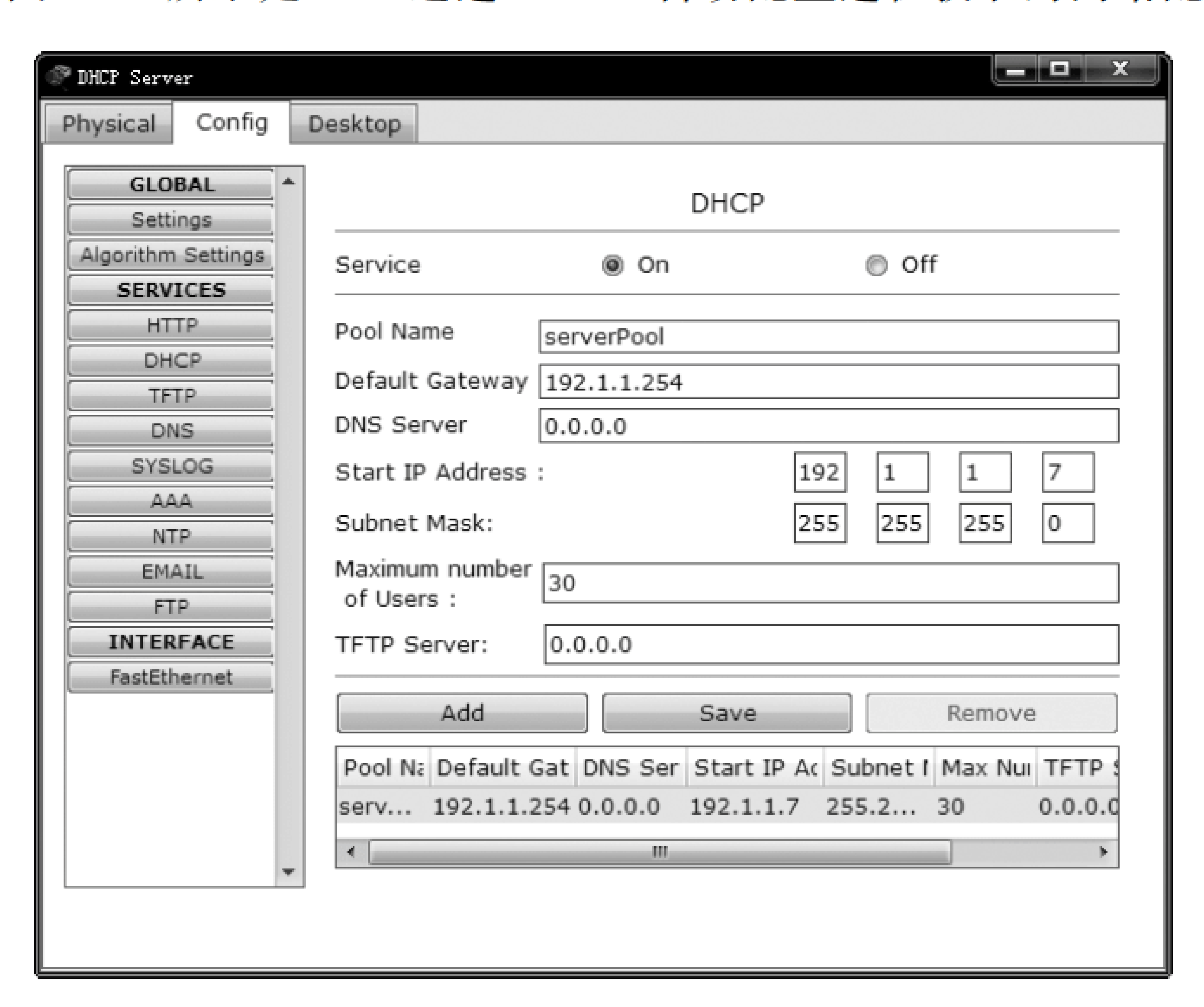


图 7.10　DHCP 服务器配置界面

(4) 为路由器接口配置 IP 地址和子网掩码。其中为连接网络 192.1.1.0/24 的接口配置 IP 地址和子网掩码 192.1.1.254/24，为连接网络 192.1.2.0/24 的接口配置 IP 地址和子网掩码 192.1.2.254/24。为 Web 服务器配置 IP 地址 192.1.2.1。

(5) 启动 PC0 实用程序 Web Browser，在地址栏中输入 Web 服务器 IP 地址 192.1.2.1，显示图 7.12 所示的 Web 服务器主页，表示 PC0 成功访问 Web 服务器。

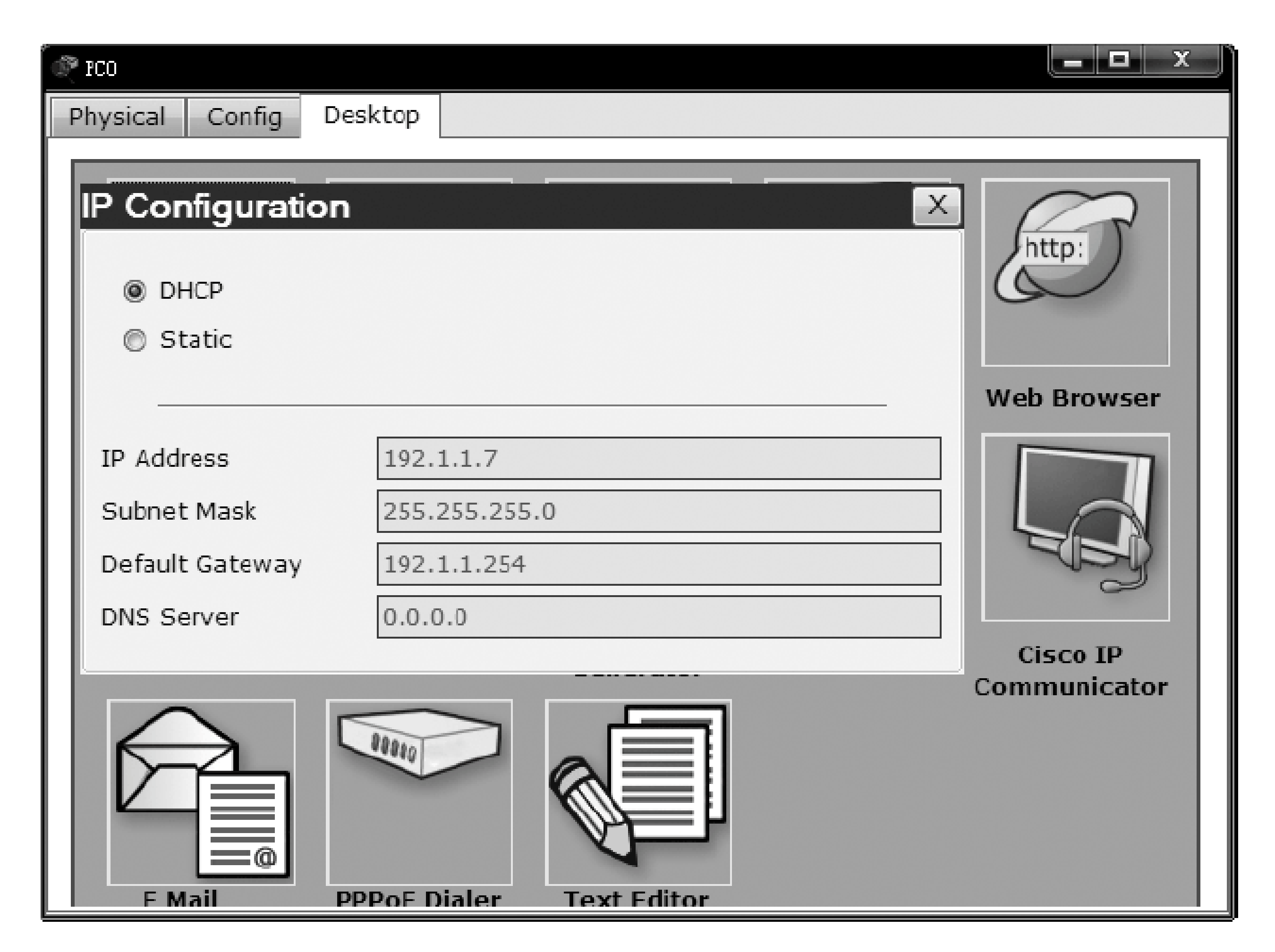


图 7.11　PC0 自动获取的网络配置信息

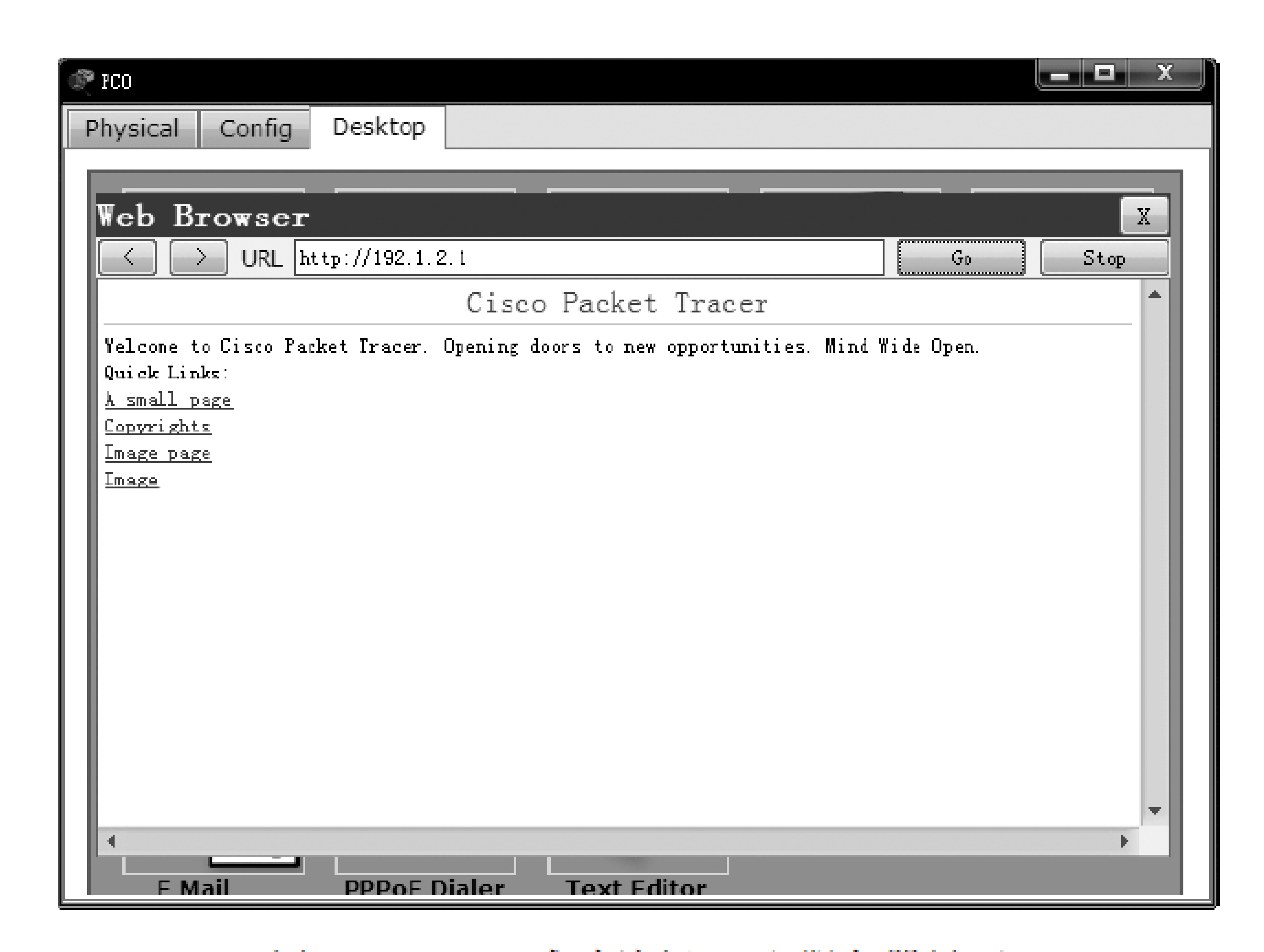


图 7.12　PC0 成功访问 Web 服务器界面

7.3.2 WPA 配置实验

1. 实验内容

(1) 完成无线局域网接入 Internet 过程。

(2) 完成终端和无线路由器的 WPA 配置。

(3) 完成无线路由器的访问控制策略配置。

(4) 验证移动终端访问 Internet 过程。

2. 网络结构

网络结构如图 7.13 所示。终端 A、B、C 和无线路由器构成一个无线内部网络，无线路由器一方面作为 AP，与内部网络无线移动终端建立关联；一方面作为边缘路由器，将无线内

部网络接入 Internet。无线路由器连接 Internet 端口配置全球 IP 地址 192.1.1.1，内部网络移动终端通过该全球 IP 地址和 PAT 实现对 Internet 的访问。由于所有内部网络移动终端发送的 IP 分组进入 Internet 后的源 IP 地址是相同的，都是全球 IP 地址 192.1.1.1，而且端口号与内部网络移动终端私有 IP 地址之间的映射是动态建立的，因此很难通过在路由器配置扩展过滤器对内部网络移动终端访问 Internet 服务器过程实施控制，需要通过在无线路由器配置访问控制策略对内部网络移动终端访问 Internet 服务器过程实施控制。

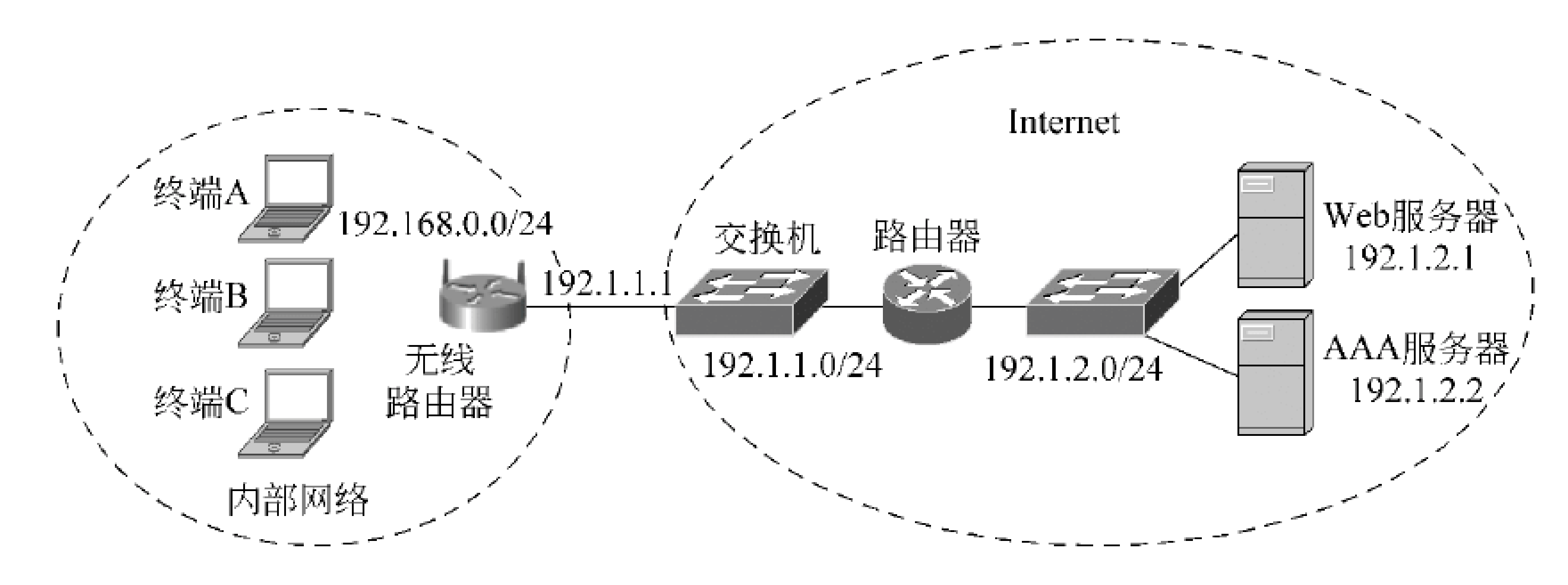


图 7.13 WPA 配置网络结构

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 7.13 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 7.14 所示。

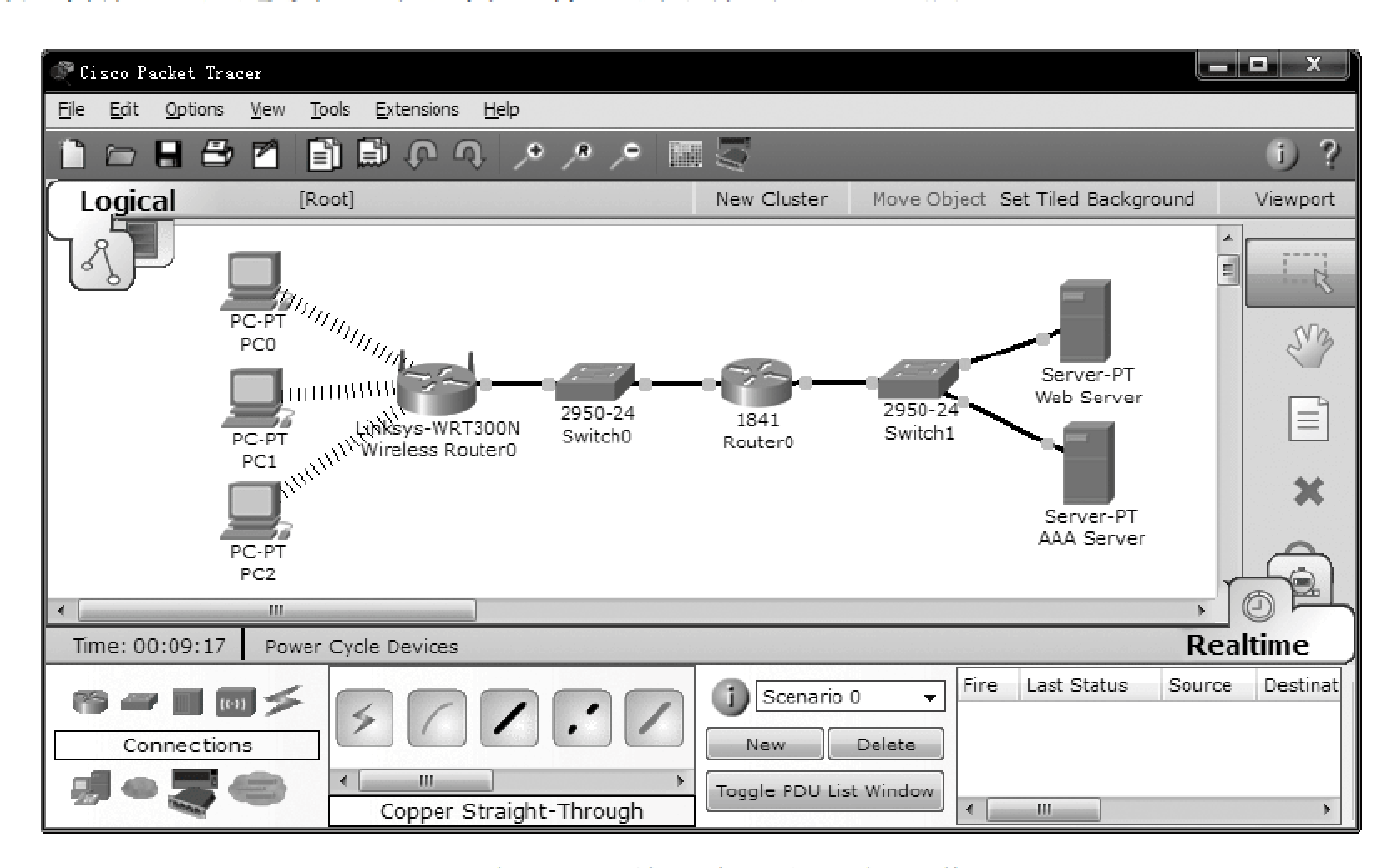


图 7.14 放置和连接设备后的逻辑工作区界面

(2) 无线路由器通过配置静态 IP 地址方式接入 Internet。这种方式下，无线路由器等同于一个接入以太网的终端，需要静态配置 IP 地址、子网掩码和默认网关地址，所配置的网络信息必须与网络地址 192.1.1.0/24 和连接该网络的路由器接口地址一致。无线路由器 Internet 接口配置界面如图 7.15 所示。

(3) 如果采用 WPA 安全协议，需要配置鉴别服务器(图 7.14 中的 AAA 服务器)，

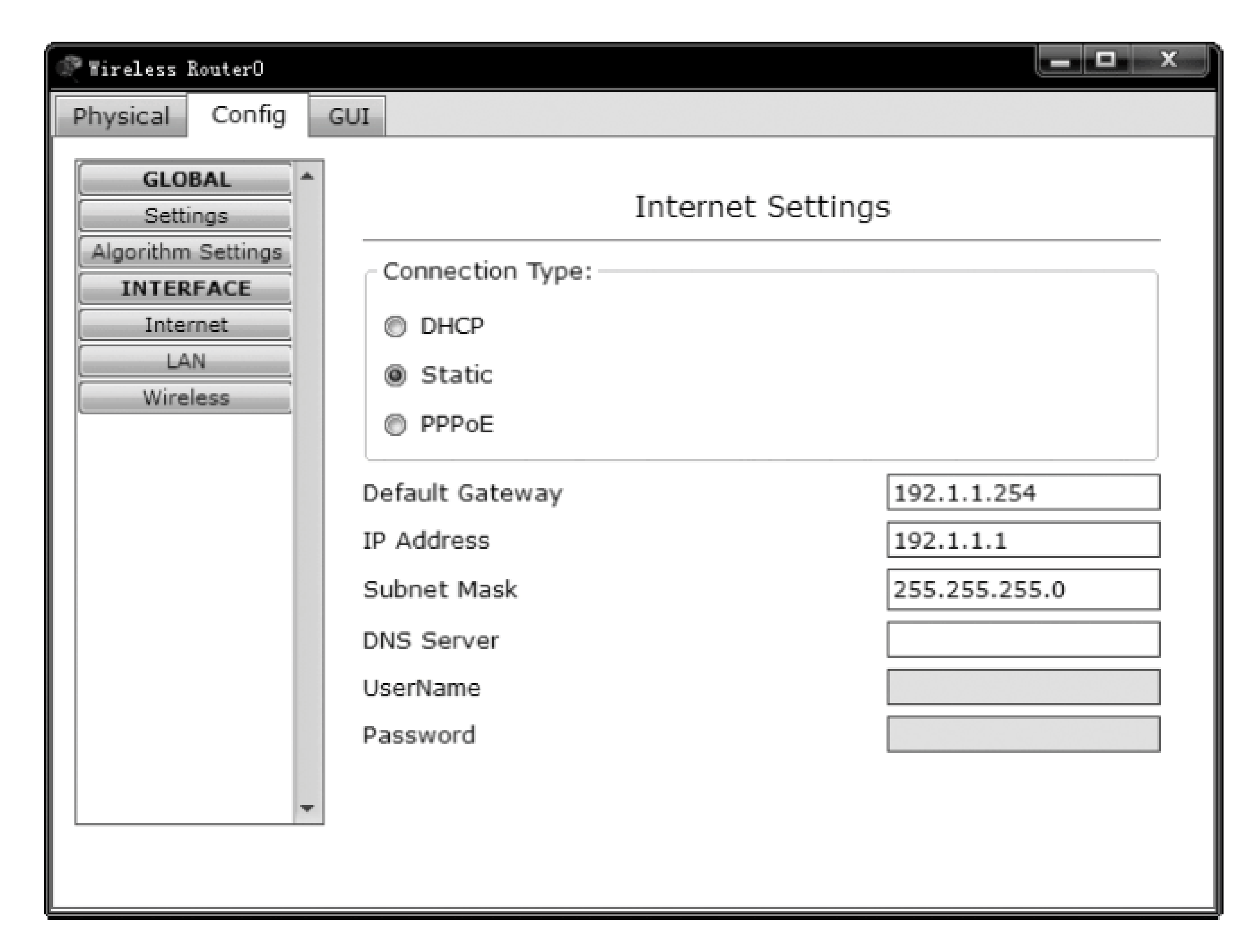


图 7.15　无线路由器 Internet 接口配置界面

AAA 服务器的网络信息配置界面如图 7.16 所示。必须在 AAA 服务器中配置有关无线路由器的信息，包括客户名(Client Name)、客户 IP 地址(Client IP)和共享密钥。由于没有为无线路由器配置主机名，客户名可以省略，客户 IP 地址为无线路由器 Internet 接口的 IP 地址，配置的共享密钥必须与无线路由器配置的共享密钥相同。用户标识信息为用户名和口令，图 7.17 中给出了用户名和口令对<aaa1，bbb1>和<aaa2，bbb2>，AAA 路由器有关 NAS 和用户的配置界面如图 7.17 所示。

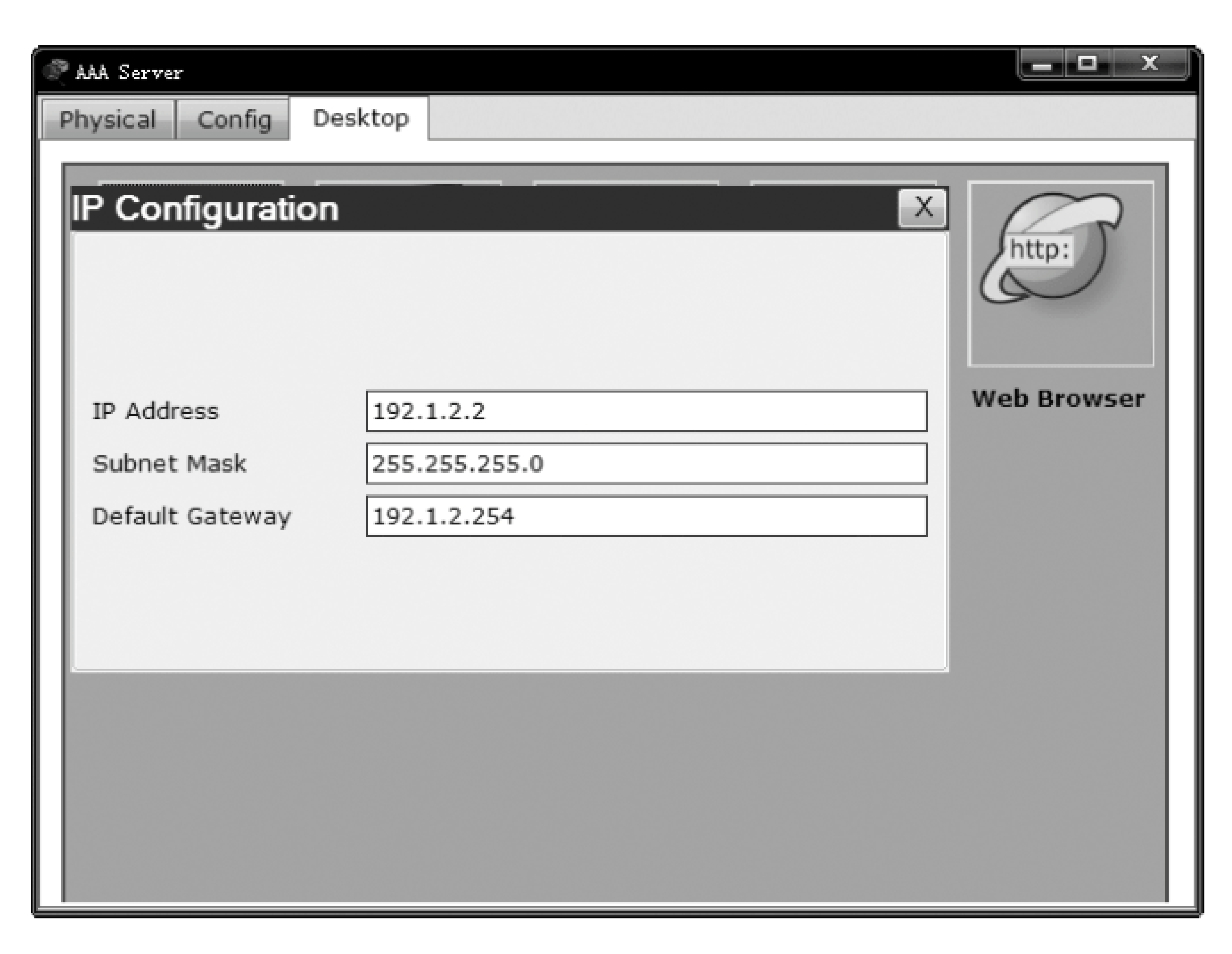


图 7.16　AAA 服务器配置的网络信息

(4) 无线路由器无线接口配置界面如图 7.18 所示。选中 WPA2 单选按钮后，出现 RADIUS 服务器 IP 地址和共享密钥输入框，IP 地址为 AAA 服务器 IP 地址 192.1.2.2，共享密钥必须与 AAA 服务器中和无线路由器关联的共享密钥相同。

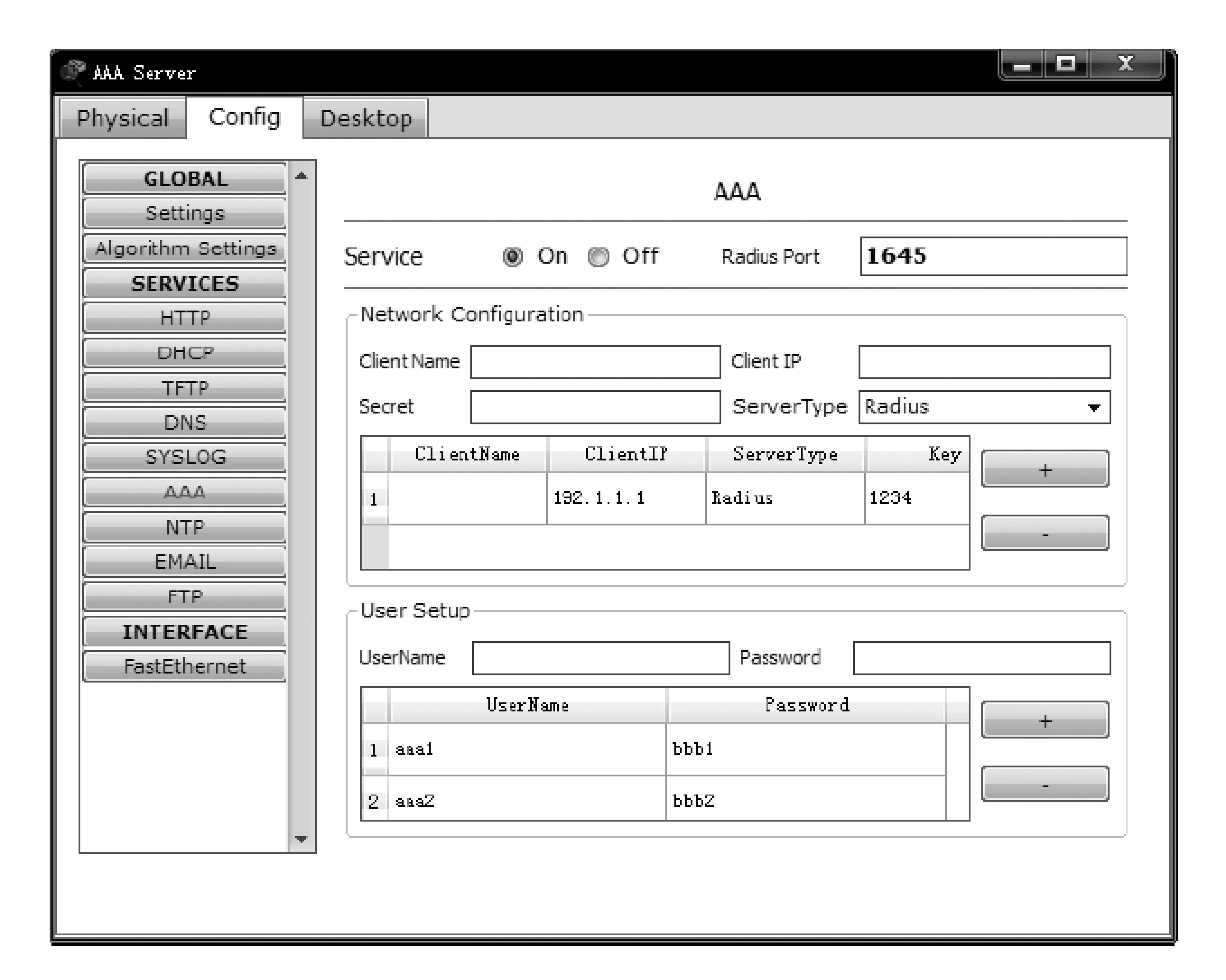


图 7.17　AAA 服务器 NAS 和用户标识信息配置界面

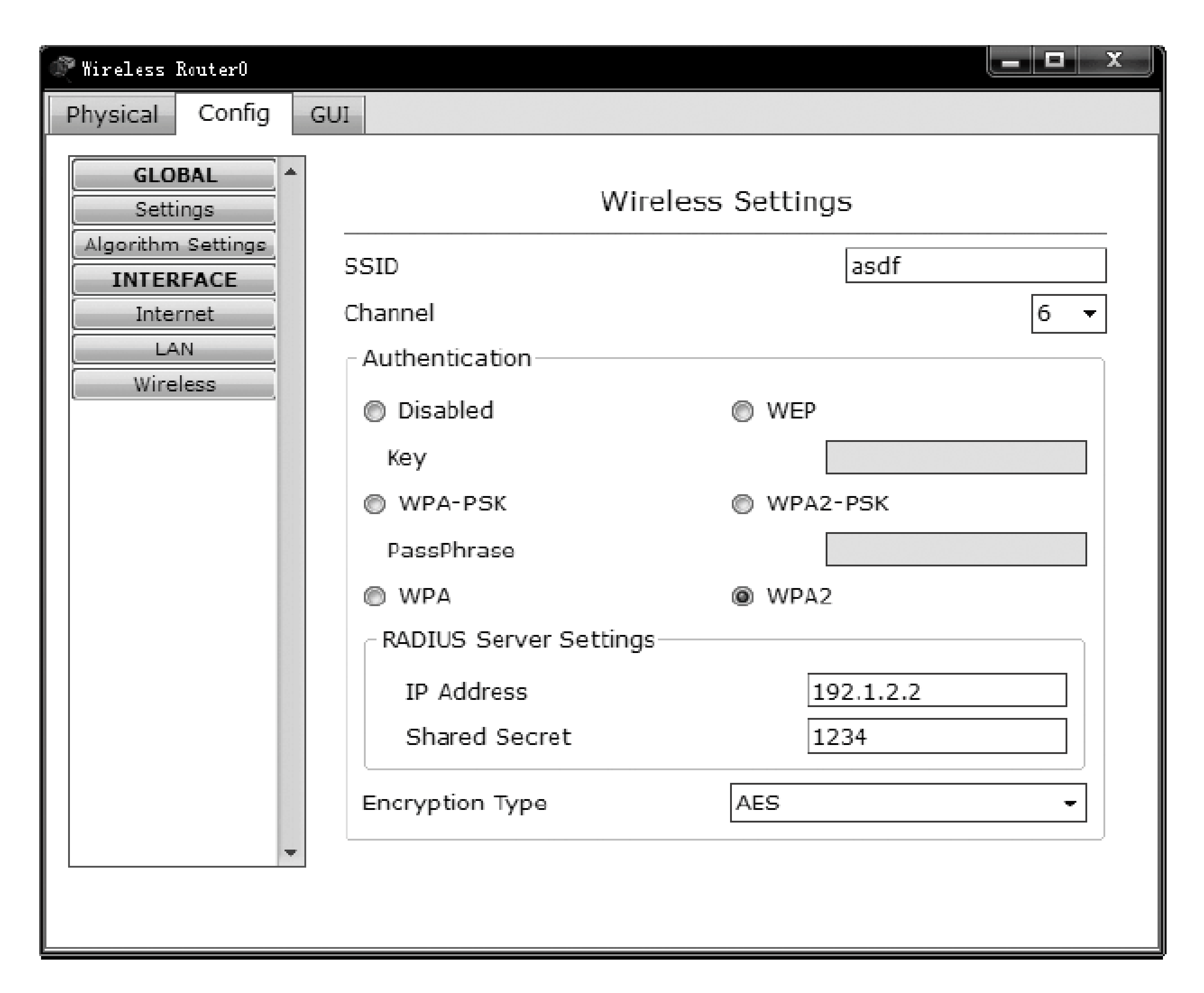


图 7.18　无线路由器无线接口配置界面

(5) 终端无线接口配置界面如图 7.19 所示。选中 WPA2 单选按钮后，出现用户名和口令输入框，输入的用户名和口令必须是 AAA 服务器中配置的用户标识信息，如 PC0 输入的用户名 aaa1 和口令 bbb1。完成 AAA 服务器、无线路由器和终端 WPA2 相关配置后，终端与无线路由器之间成功建立关联，图 7.14 是终端与无线路由器成功建立关联后的示意图。

(6) 无线路由器本身是一个 DHCP 服务器，内部网络移动终端通过 DHCP 自动配置过程获取网络信息。在为路由器接口配置 IP 地址和子网掩码后，内部网络移动终端可以访问 Internet 服务器，图 7.20 是 PC0 成功访问 Web 服务器界面。

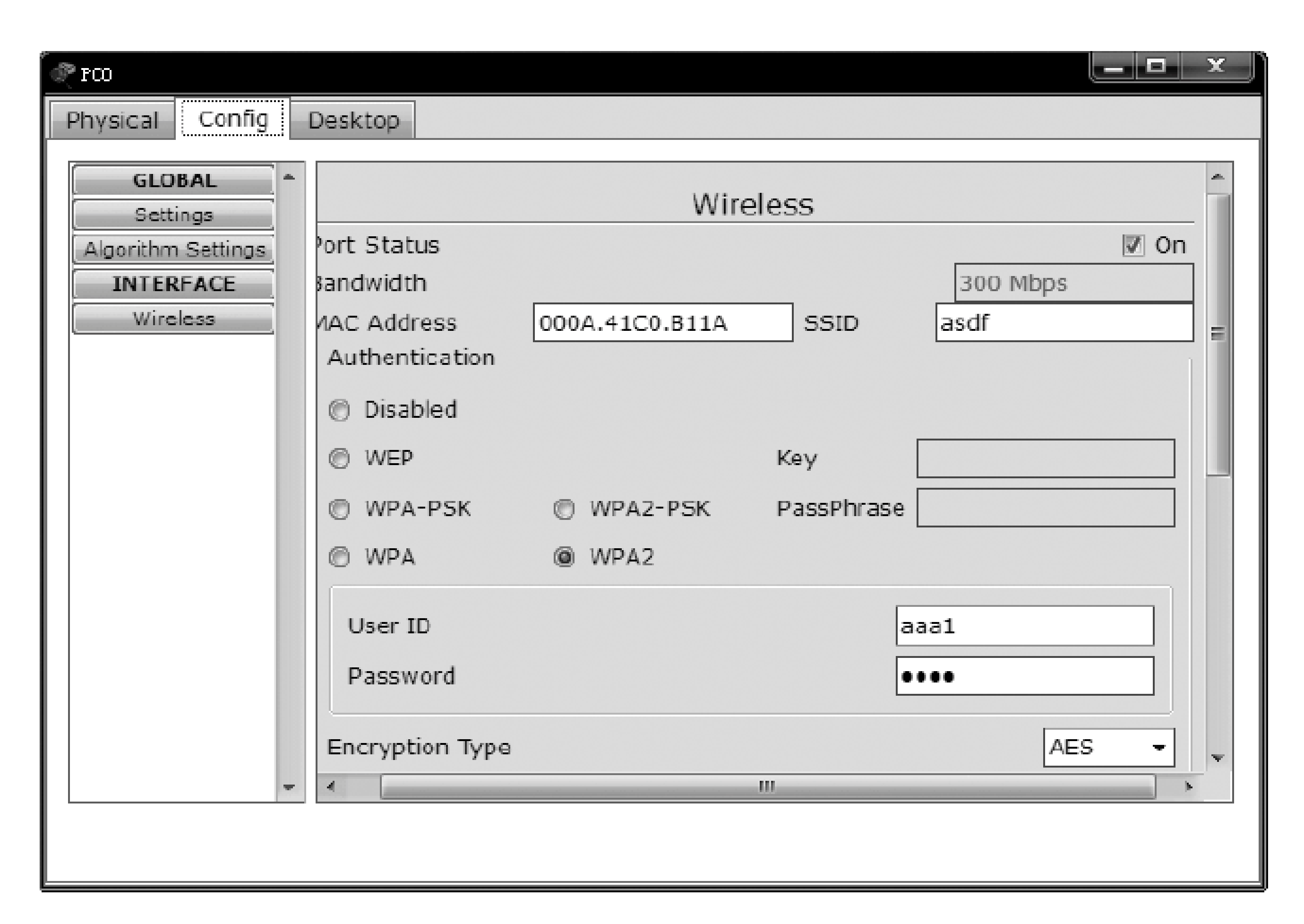


图 7.19 PC0 无线接口配置界面

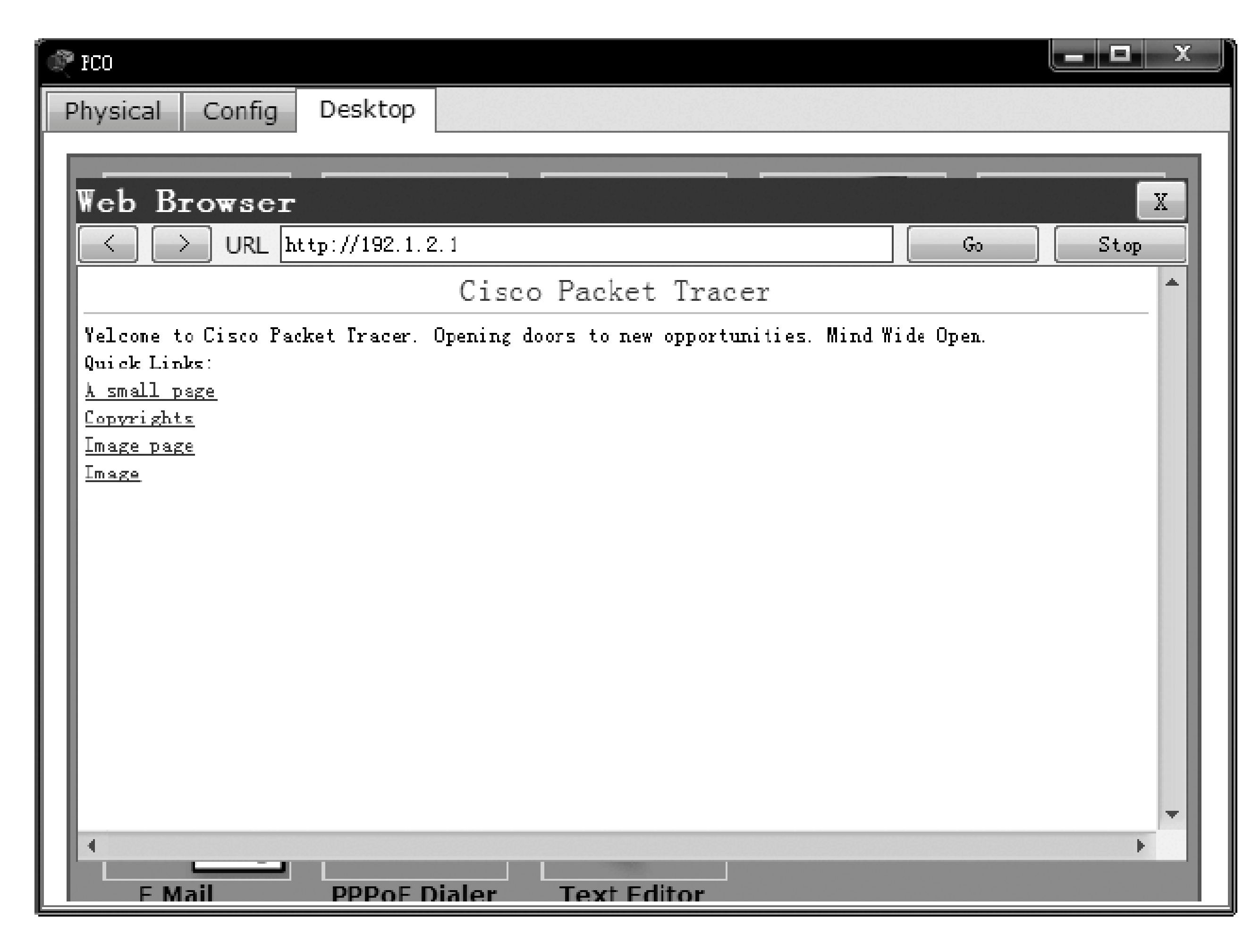


图 7.20 PC0 成功访问 Web 服务器界面

(7) 在 PC0、PC1 和 PC2 访问 Web 服务器后，无线路由器的 NAT 表内容如图 7.21 所示，虽然三项和 TCP 连接关联的映射中，本地全球信息中的全球 IP 地址是相同的，但用本地全球信息中内部网络唯一的端口号 1024、1025 和 1026 绑定内部网络私有地址 192.168.0.100、192.168.0.102 和 192.168.0.101。与 UDP 关联的映射是无线路由器访问 AAA 服务器时建立的。

NAT Table for Wireless Router0

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
tcp	192.1.1.1:1024	192.168.0.100:1025	192.1.2.1:80	192.1.2.1:80
tcp	192.1.1.1:1025	192.168.0.102:1025	192.1.2.1:80	192.1.2.1:80
tcp	192.1.1.1:1026	192.168.0.101:1025	192.1.2.1:80	192.1.2.1:80
udp	192.1.1.1:1645	192.1.1.1:1645	192.1.2.2:1645	192.1.2.2:1645

图 7.21 无线路由器 NAT 表

(8) 如果要禁止内部网络中私有 IP 地址为 192.168.0.101 的移动终端访问 FTP 服务器(图 7.14 中的 Web 服务器同时又是 FTP 服务器),在无线路由器访问控制菜单下单击 Edit List(编辑列表)按钮,在出现的 IP 地址输入框中输入 IP 地址 192.168.0.101,如图 7.22 所示。在访问控制菜单下将应用层协议 FTP 移到阻塞列表中,如图 7.23 所示。单击访问控制菜单下的 Save Settings(保存设置)按钮,完成无线路由器访问控制策略配置。

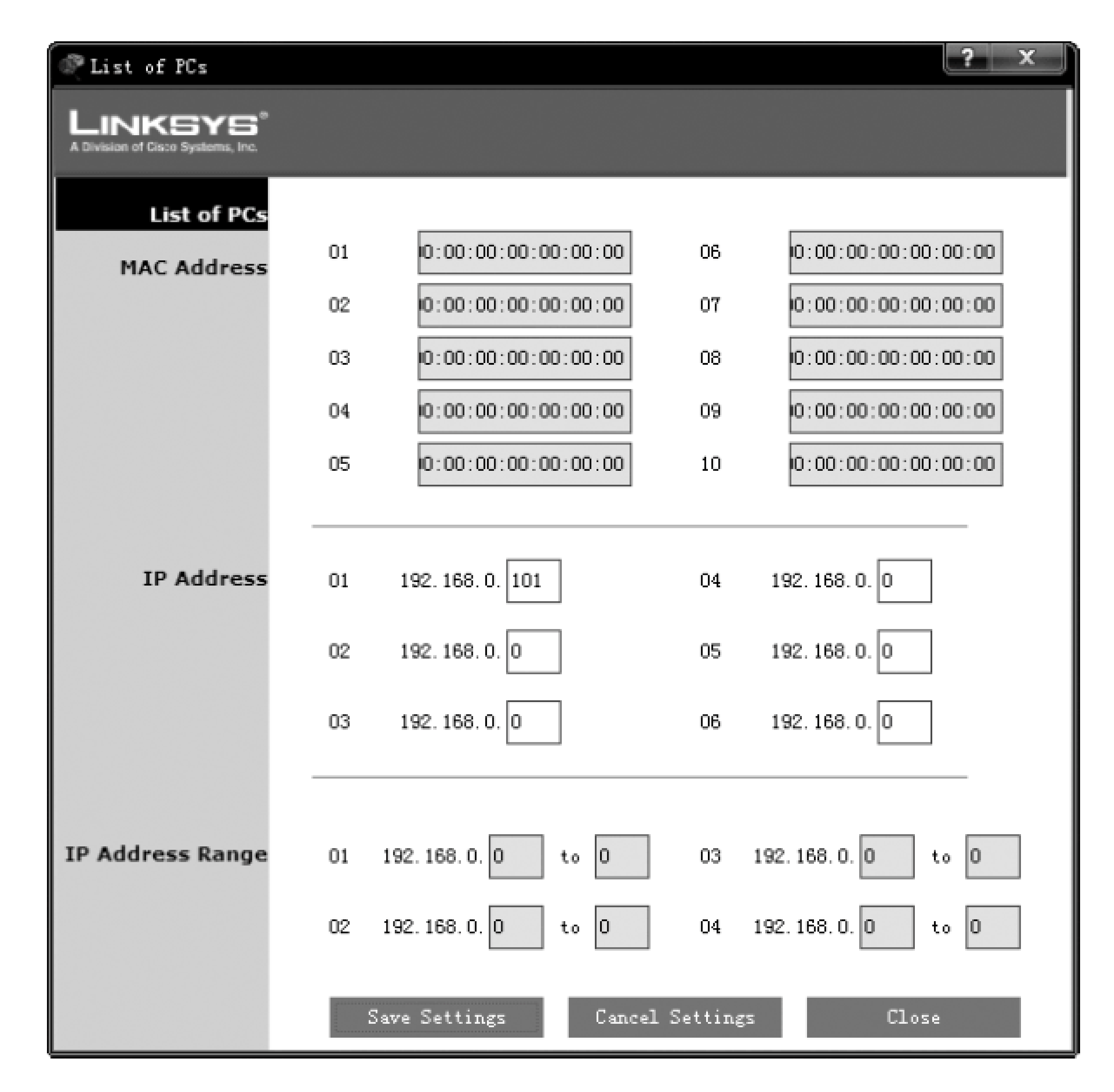


图 7.22　设置访问控制策略中内部网络移动终端的私有 IP 地址

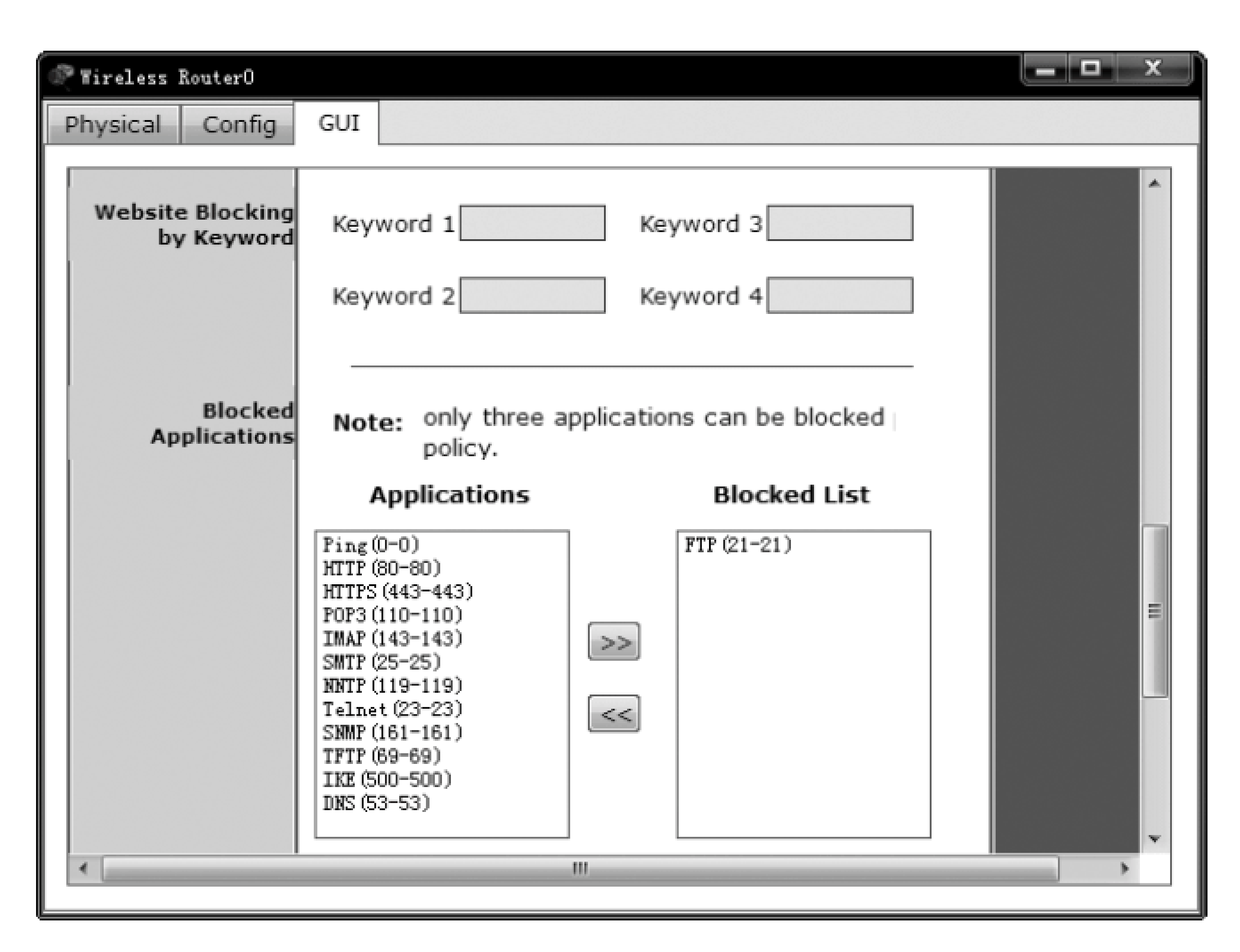


图 7.23　配置访问控制策略需要阻塞的应用层协议

(9) 由于 PC0 的内部网络私有 IP 地址不是 192.168.0.101,因而可以访问 FTP 服务器,图 7.24 是 PC0 成功访问 FTP 服务器界面。PC2 的内部网络信息如图 7.25 所示,由于它的内部网络私有地址是 192.168.0.101,因而无法访问 FTP 服务器。图 7.26 是 PC2 访问 FTP 服务器失败的界面。

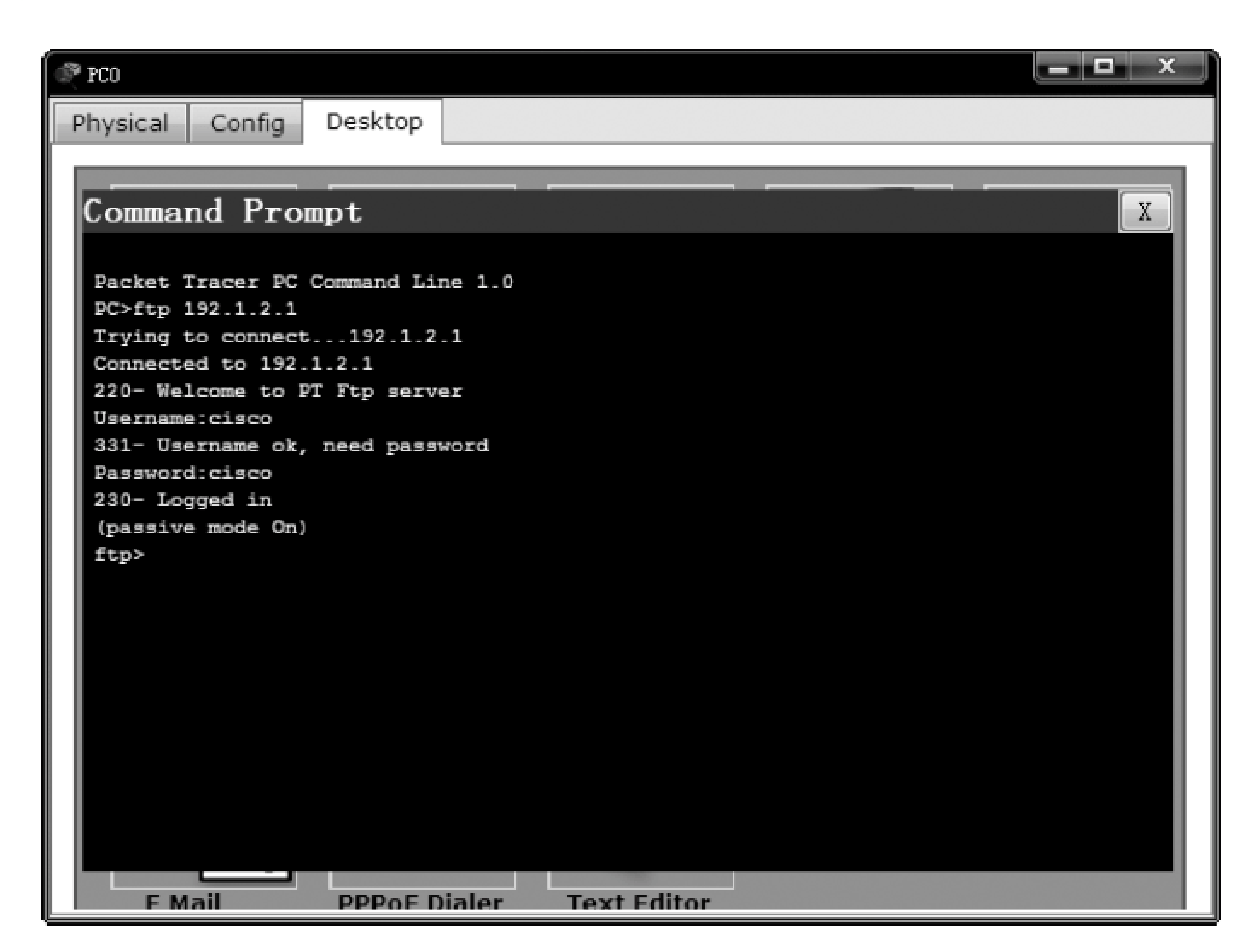


图 7.24 PC0 成功访问 FTP 服务器界面



图 7.25 PC2 网络信息配置界面

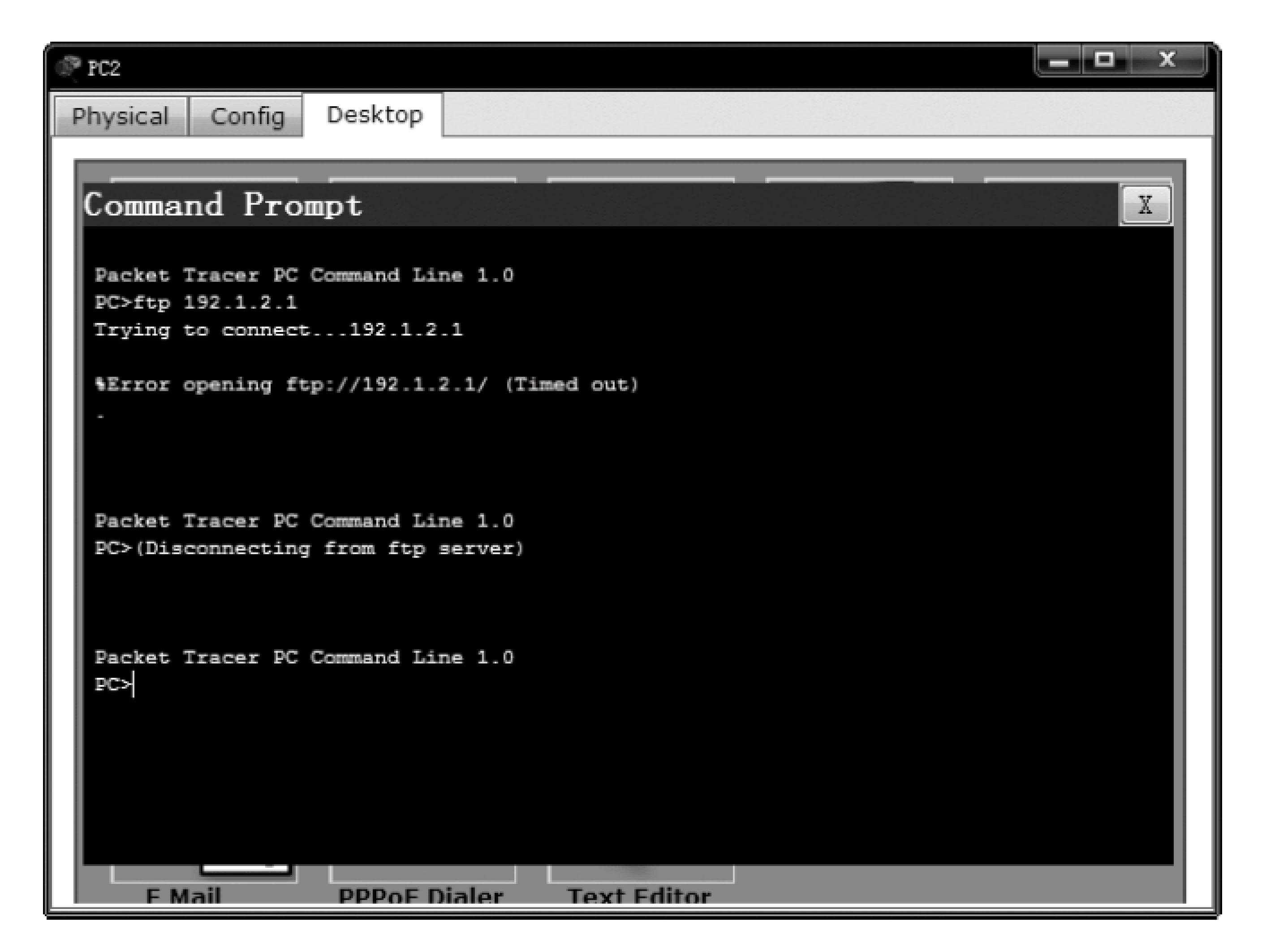


图 7.26　PC2 访问 FTP 服务器失败界面

第 8 章 CHAPTER

虚拟专用网络

8.1 知识要点

8.1.1 点对点 IP 隧道

1. 网络结构

虚拟专用网络与前面讨论的通过 NAT 实现内部网络和公共网络互连不同，它将通过公共网络互连在一起的多个内部网络视为一个整体，就像是一个由专用物理链路互连多个子网构成的企业网，属于不同内部网络的终端之间直接可以通过本地 IP 地址相互通信，不同内部网络需要分配不同的本地 IP 地址。对于内部网络中的终端，公共网络是透明的。

互连内部网络和公共网络的路由器称为边缘路由器，图 8.1 中的路由器 R1、R2 和 R3 就是边缘路由器，边缘路由器的作用是创建实现不同内部网络互连的点对点 IP 隧道。从内部网络的角度看，边缘路由器的作用就是通过点对点 IP 隧道实现多个不同的内部网络的互连，点对点 IP 隧道等同于专用点对点物理链路。从公共网络的角度看，边缘路由器的作用是实现和公共网络互连，并通过公共网络建立边缘路由器连接公共网络接口之间的 IP 分组传输路径。

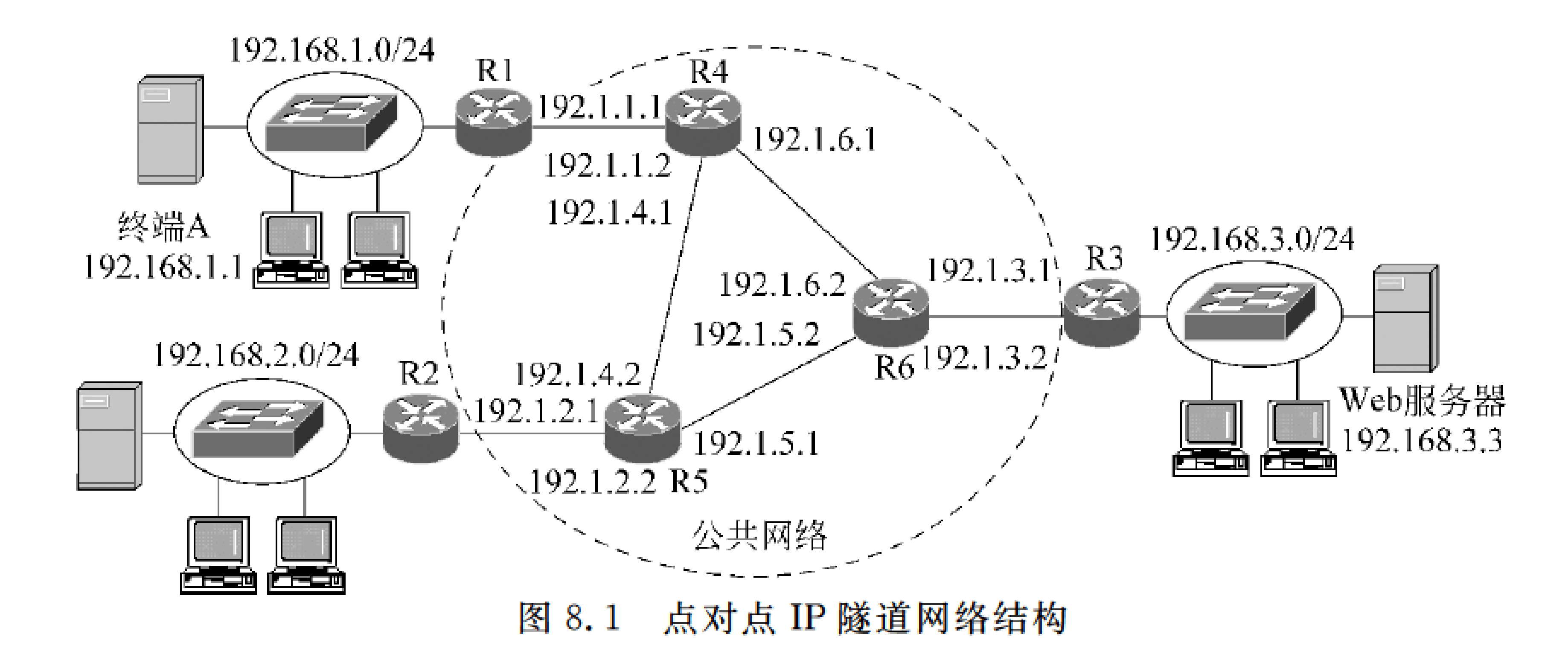


图 8.1 点对点 IP 隧道网络结构

VPN 存在两层 IP 分组传输路径：一层是图 8.2 所示的内部网络之间的 IP 分组传输路径，在这一层传输路径中，公共网络的功能被定义为实现边缘路由器之间 IP 分组传输的点对点 IP 隧道。另一层是公共网络中边缘路由器连接公共网络接口之间的 IP 分组传输路径，如图 8.1 中 R1 全球 IP 地址为 192.1.1.1 的接口和 R2 全球 IP 地址为 192.1.2.1 的接口之间的 IP 分组传输路径。这一层传输路径是实现点对点 IP 隧道的基础，但对内部网络中的终端是透明的。

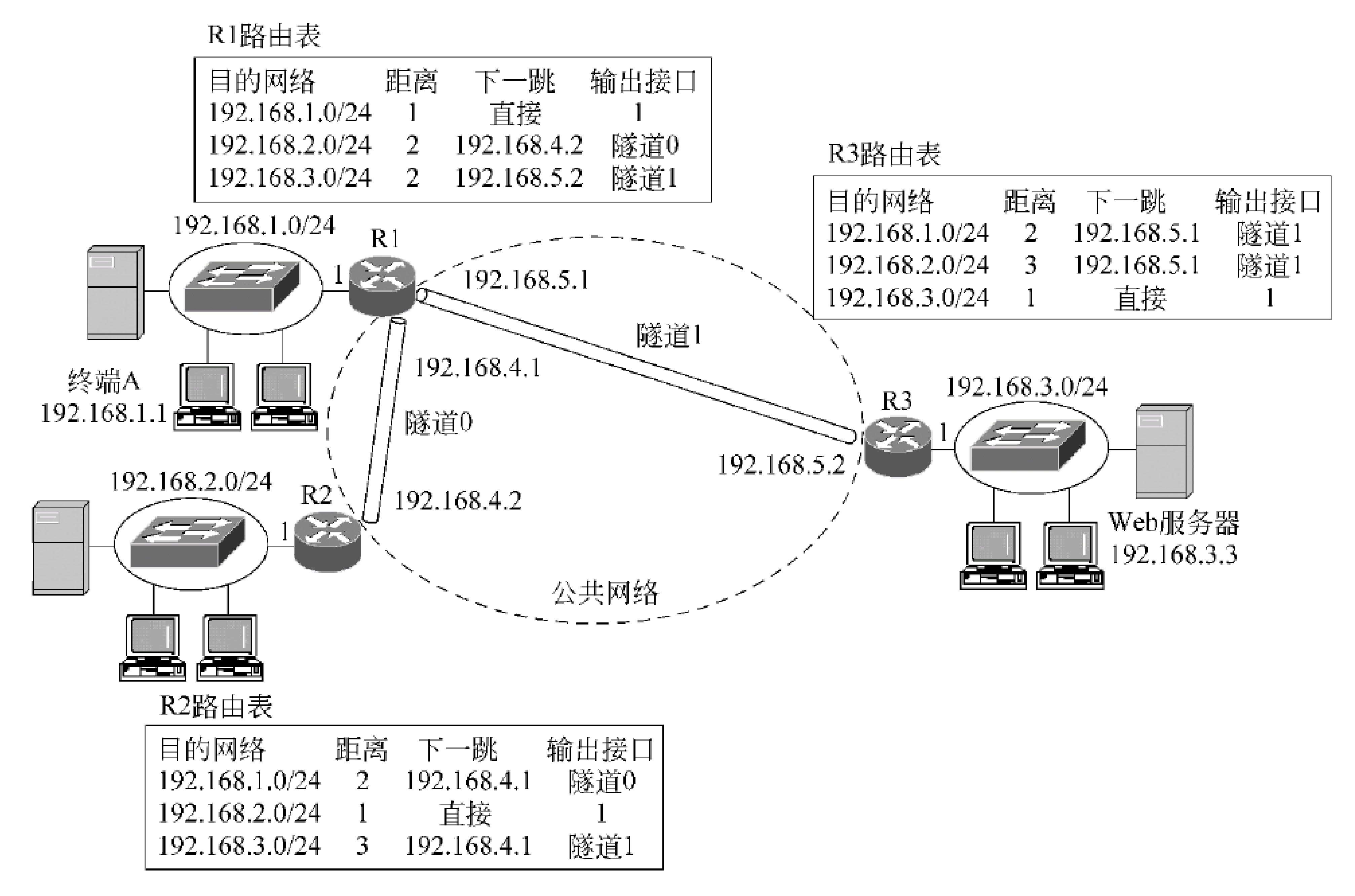


图 8.2 内部网络逻辑结构

2. GRE 和 IP-in-IP

(1) GRE

一般路由封装(Generic Routing Encapsulation，GRE)是一种经过点对点 IP 隧道传输多种不同协议数据单元的协议，其封装过程如图 8.3 所示。如果需要经过点对点 IP 隧道传输的协议数据单元是一个 IP 分组，则称其为内层 IP 分组。内层 IP 分组被封装成 GRE 格式，通过类型字段 0x800 表明协议数据单元是 IP 分组，GRE 类型字段取值与以太网 MAC 帧类型字段取值一致。GRE 格式被封装成 IP 隧道格式，IP 隧道格式其实就是以点对点 IP 隧道两端 IP 地址为源和目的 IP 地址的 IP 分组，通过协议字段值 47 表明净荷为 GRE 格式。IP 隧道格式也称为外层 IP 分组。图 8.1 中终端 A 传输给 Web 服务器的 IP 分组经过图 8.2 中隧道 1 传输时，被封装成图 8.3 所示的外层 IP 分组格式。

(2) IP-in-IP

IP-in-IP 直接将 IP 分组作为另一个 IP 分组的净荷，用协议字段值 4 表明 IP 分组净荷是一个完整的 IP 分组。作为净荷的 IP 分组往往是内部网络终端之间传输的 IP 分组，以内部网络本地 IP 地址为源和目的 IP 地址，该 IP 分组也称为内层 IP 分组，封装内层 IP

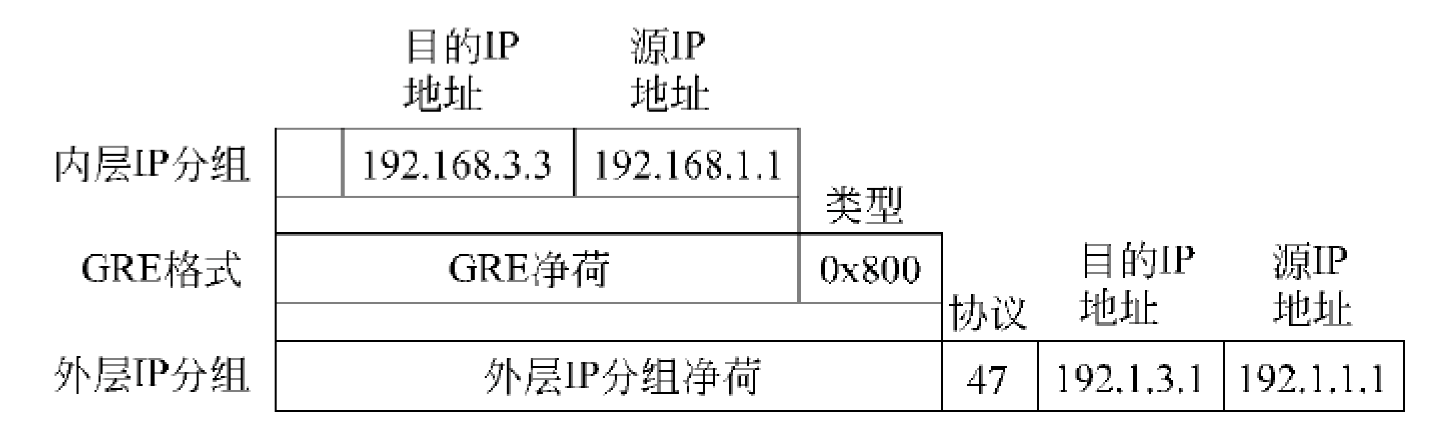


图 8.3 GRE 封装过程

分组的 IP 分组称为外层 IP 分组,用于实现内层 IP 分组点对点 IP 隧道一端至另一端传输过程,因此,外层 IP 分组以点对点 IP 隧道两端 IP 地址为源和目的 IP 地址。图 8.1 中终端 A 传输给 Web 服务器的 IP 分组经过图 8.2 中隧道 1 传输时,被封装成图 8.4 所示的 IP-in-IP 格式。

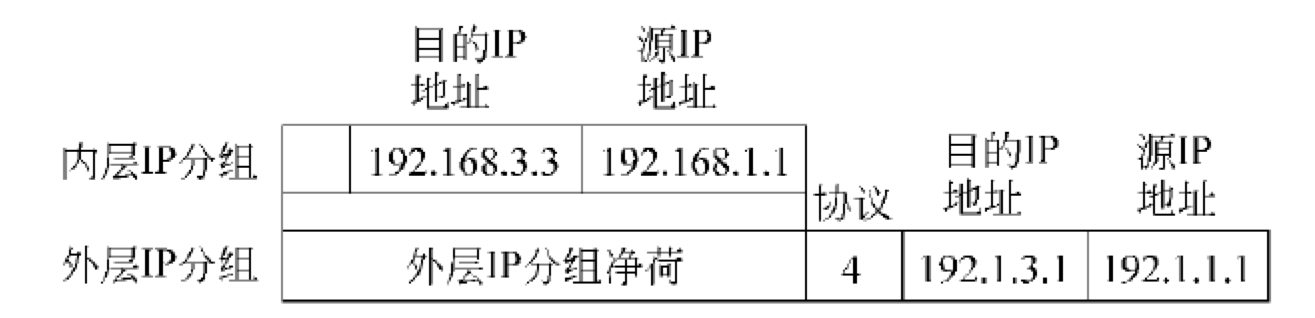


图 8.4 IP-in-IP 格式

3. IP 隧道建立过程

一是配置隧道,主要配置隧道两端的全球 IP 地址,因此隧道两端必须是连接公共网络的路由器接口,如图 8.1 中路由器 R1 和 R3 连接公共网络的接口。由于图 8.2 中隧道 1 两端对应图 8.1 中路由器 R1 和 R3 连接公共网络的接口,因此创建隧道 1 时,需为隧道 1 两端配置全球 IP 地址 192.1.1.1 和 192.1.3.1。同时可以为隧道两端配置内部网络本地 IP 地址,如图 8.2 中为隧道 1 两端配置的内部网络本地 IP 地址 192.168.5.1 和 192.168.5.2。在通过路由协议建立用于指明通往内部网络各个子网的路由项时,路由项中的下一跳地址是为隧道两端配置的内部网络本地 IP 地址。二是公共网络必须建立隧道两端之间的传输路径,隧道两端通过 GRE Keepalive 报文检测隧道两端的连通性,对于内部网络而言,隧道两端之间的连通性等于互连边缘路由器的物理链路的有效性,一旦某个隧道两端之间无法连通,就像边缘路由器的某个接口关闭,该隧道直接连接的内部网络子网和通过该隧道到达的目的网络都从路由表中删除。

公共网络建立隧道两端之间的传输路径时,内部网络对公共网络中的路由器是透明的。边缘路由器是唯一既参与建立内部网络各个子网之间传输路径,又参与建立公共网络中隧道两端之间传输路径的路由器,但必须用不同的路由协议进程。

4. 数据传输过程

创建隧道,并建立边缘路由器用于指明通往内部网络中各个子网的传输路径的路由项后,可以进行内部网络中两个终端之间的通信过程,如图 8.2 中终端 A 和 Web 服务器之间的通信过程。终端 A 的默认网关是边缘路由器 R1,当终端 A 向 Web 服务器发送 IP 分组时,创建源 IP 地址为终端 A 本地 IP 地址 192.168.1.1,目的 IP 地址为 Web 服务器本地 IP 地址 192.168.3.3 的内层 IP 分组,并将内层 IP 分组发送给默认网关——边缘路

由器 R1,R1 通过检索路由表确定通过隧道 1 将内层 IP 分组传输给下一跳,将该内层 IP 分组封装成隧道 1 对应的格式,根据隧道 1 的配置,隧道 1 是两端全球 IP 地址分别是 192.1.1.1 和 192.1.3.1 的点对点 IP 隧道,将该内层 IP 分组封装成图 8.3 所示的外层 IP 分组格式,实际上就是点对点 IP 隧道格式。外层 IP 分组经过公共网络建立的隧道 1 两端之间的传输路径到达边缘路由器 R3,R3 从隧道 1 对应的封装格式中分离出内层 IP 分组,将其提交给 R3 的路由进程,R3 路由进程确定目的终端直接连接在接口 1 连接的以太网上,将该内层 IP 分组封装成 MAC 帧,通过互连 R3 接口 1 和 Web 服务器的以太网将该内层 IP 分组传输给 Web 服务器,完成该内层 IP 分组终端 A 至 Web 服务器的传输过程。

8.1.2 IP Sec 和 VPN

隧道解决了通过公共网络互连的内部网络各个子网之间的通信问题,但隧道本身不具有安全传输功能,不能保证经过公共网络传输的数据的保密性和完整性。实现经过公共网络传输的数据的安全性和保密性的机制是 IP Sec,IP Sec 和点对点 IP 隧道的有机结合实现公共网络互连的内部网络各个子网之间的安全通信。

1. IP Sec

IP Sec 包含 AH 和 ESP,AH 保证经过公共网络传输的数据的完整性,ESP 保证经过公共网络传输的数据的保密性和完整性。保密性通过加密算法实现,IP Sec 支持对称密钥加密算法 DES、3DES 和 AES 等;完整性通过散列消息鉴别码(Hashed Message Authentication Codes ,HMAC)实现,IP Sec 支持 HMAC-MD5 和 HMAC-SHA 等 HMAC 算法。隧道两端之间通过 IP Sec 实现安全通信前,必须约定加密算法和加密密钥、HMAC 算法和鉴别密钥。两端通过建立安全关联完成相关参数的约定过程。

2. 安全关联建立过程

可以通过在隧道两端人工配置相关参数完成安全关联建立过程,也可以通过 Internet 安全关联和密钥管理协议(Internet Security Association and Key Management Protocol,ISAKMP)动态建立安全关联。ISAKMP 建立安全关联分为两个阶段:第一个阶段用于建立安全传输通道,主要完成加密算法、报文摘要算法、密钥交换协议的约定,完成密钥交换过程,鉴别两端身份。第二个阶段通过第一阶段建立的安全传输通道实现 ISAKMP 消息的安全传输,并因此完成安全关联的建立过程。双方在建立安全关联过程中完成安全协议(AH 或 ESP)、对称密钥加密算法(DES、3DES 或 AES)和 HMAC 算法(HAMC-MD5 或 HMAC-SHA)的约定,密钥一般使用第一阶段通过密钥交换过程生成的密钥。

(1) 第一阶段。

完成第一阶段的前提是双方具有匹配的 ISAKMP 策略,即双方支持的加密算法、报文摘要算法、密钥交换协议和鉴别方式存在交集。假定图 8.2 中隧道 1 两端配置的 ISAKMP 策略如表 8.1 所示,两端可以完成第一阶段。第一阶段工作过程如图 8.5 所示。

表 8.1　隧道 1 两端配置的 ISAKMP 策略

匹配项目	Router1	Router3
鉴别方式	共享密钥，密钥为 PSK	共享密钥，密钥为 PSK
加密算法	3DES	3DES
报文摘要算法	MD5	MD5
密钥交换方式	DH 组 2	DH 组 2
对方标识信息	192.1.3.1	192.1.1.1

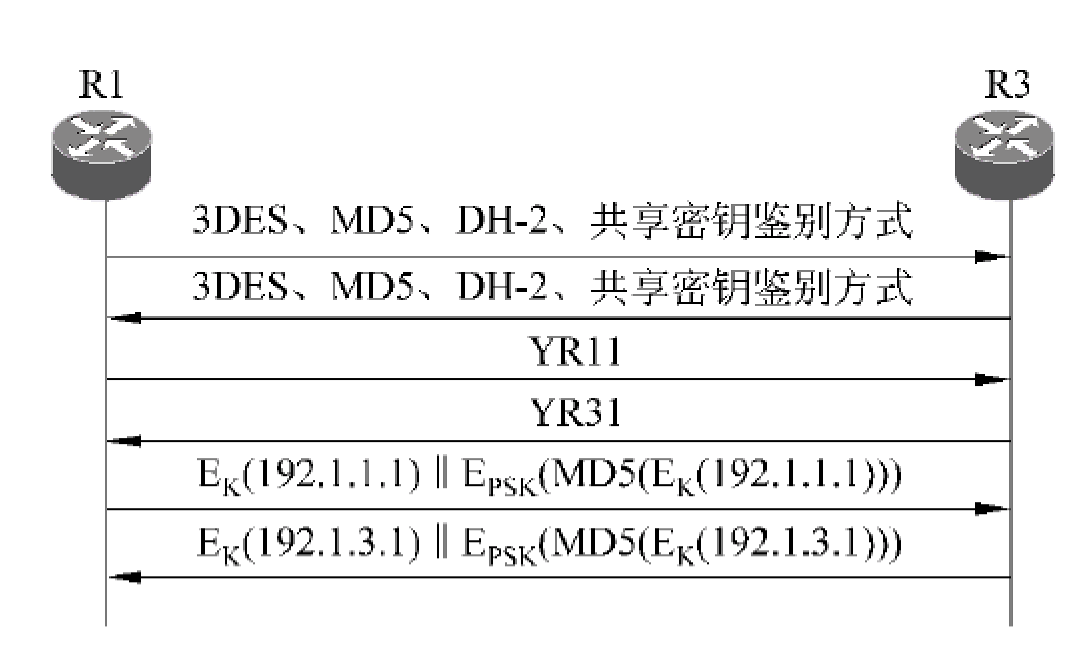


图 8.5　第一阶段工作过程

第一阶段总共有三次交换过程，第一次交换过程确定双方采用的算法和鉴别方式，两端支持的算法和鉴别方式必须存在交集，否则终止安全关联建立过程。通过第一次交换过程确定双方认可的算法和鉴别方式。

第二次交换过程用于交换根据 DH-2 生成密钥需要的参数。双方选择 DH-2 等同于确定了原根 α 和大素数 p，Router1 选择一个小于 p 的随机整数 XR11，使得 $YR11=\alpha^{XR11} \bmod p$，将 XR11 保留，将 YR11 传输给 Router3。同样，Router3 选择一个小于 p 的随机整数 XR31，使得 $YR31=\alpha^{XR31} \bmod p$，将 XR31 保留，将 YR31 传输给 Router1。Router1 和 Router3 求出密钥 $K=YR31^{XR11} \bmod p= YR11^{XR31} \bmod p$。

第三次交换过程一是验证第一、第二次交换过程中所传输消息的完整性；二是鉴别两端身份。用第一次交换过程确定的加密算法和第二次交换过程求出的密钥 K 加密各端自身标识符，如 Router1 发送的密文 $E_K(192.1.1.1)$ 和根据密文计算出的鉴别信息 $E_{PSK}(MD5(E_K(192.1.1.1)))$，Router3 在顺利完成下述操作的情况下通过对 Router1 的身份鉴别，一是必须能够解密出 Router1 标识信息，并确定和配置的 Router1 标识信息相同；二是能够用鉴别信息验证密文的完整性。完成第一项操作表示双方有着相同的加密算法、DH 组号，并成功完成了第二次交换过程。完成第二项操作表示双方有着相同的共享密钥 PSK、相同的报文摘要算法。配置 Router3 时，将共享密钥 PSK 和标识符 192.1.1.1 绑定，以此表明拥有共享密钥 PSK 的一端是标识符为 192.1.1.1 的一端。Router1 通过同样的操作完成对 Router3 的身份鉴别。

(2) 第二阶段。

第二阶段工作过程与第一阶段相似，首先必须双方配置相同的 IP Sec 参数，如 ESP-

3DES 和 ESP-MD5-HMAC，表示采用 ESP 协议，加密算法是 3DES，HMAC 算法是 HMAC-MD5。通常第二阶段通过一次交换过程和三个报文实现，如图 8.6 所示。这三个报文用于完成以下三个功能：一是确定双方支持的安全协议和加密、HMAC 算法；二是交换用于产生密钥的参数；三是验证交换过程的完整性，并实现源端鉴别。

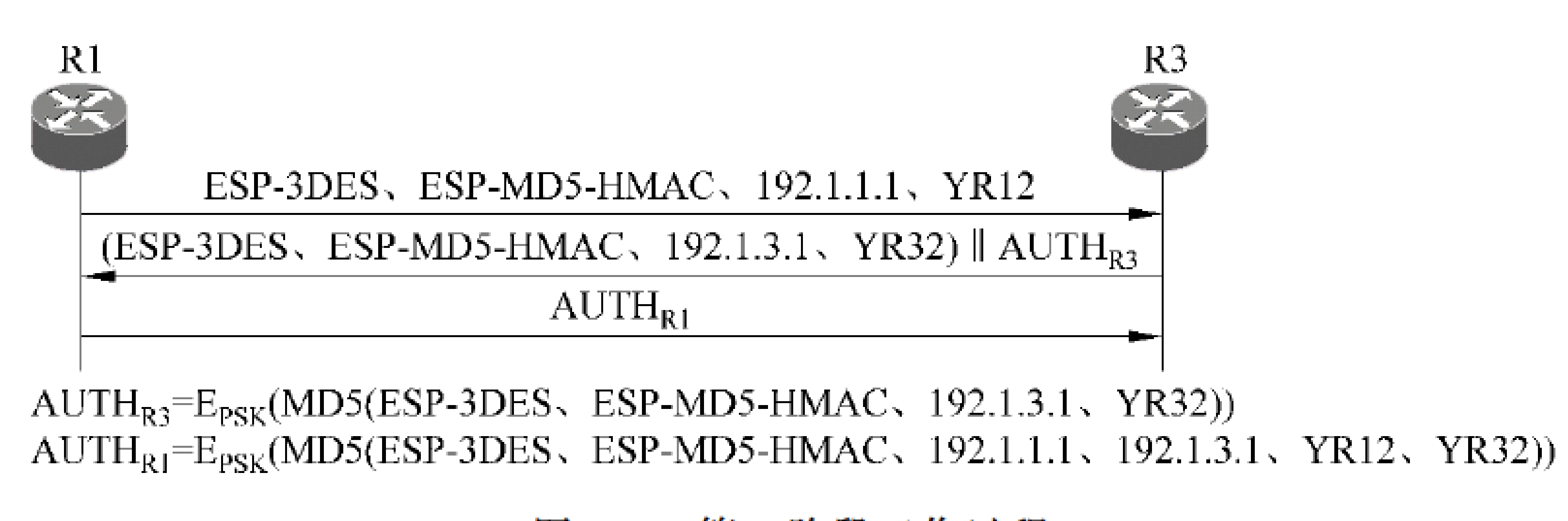


图 8.6 第二阶段工作过程

由于完成第一阶段工作过程后双方已经约定了加密算法和密钥，因此在第二阶段工作过程中，一是可以通过加密传输来保证某些数据的保密性；二是可以采用第一阶段工作过程中计算出的密钥作为 ESP 加密密钥和 HMAC 密钥，无须在第二阶段交换有关产生密钥的参数。

3. ESP 封装过程

一旦隧道 1 建立 Router1 至 Router3 安全关联，经过隧道 1 传输的图 8.2 中终端 A 至 Web 服务器的内层 IP 分组封装过程如图 8.7 所示。内层 IP 分组首先被封装成 GRE 格式，内层 IP 分组作为 GRE 格式的净荷，GRE 格式用类型字段值 0x800 表明这一点。GRE 格式被封装成 ESP 报文，GRE 格式作为 ESP 报文净荷，ESP 报文用 ESP 首部中下一个首部字段值 0x2f(十进制值 47)表明这一点。对 ESP 报文中的净荷和尾部用 3DES 加密算法进行加密运算，加密密钥 K1 通过图 8.6 中的参数 YR12 和 YR32 计算所得。对 ESP 首部和加密运算后得到的密文用 HAMC-MD5 计算消息鉴别码，取计算所得消息鉴别码的高 96 位作为 ESP 报文的消息鉴别码。HMAC 密钥 K2 同样通过图 8.6 中的参数 YR12 和 YR32 计算所得。将 ESP 报文封装成外层 IP 分组，ESP 报文作为外层 IP 分组净荷，外层 IP 分组用首部中协议字段值 0x32(十进制值 50)表明这一点。实际经过隧道 1 传输的是图 8.7 所示的外层 IP 分组。

8.1.3 Cisco Easy VPN

1. 网络结构

Cisco Easy VPN 用于解决连接在 Internet 上的终端访问内部网络资源的问题。图 8.8 给出了用于实现远程接入的网络结构。内部网络由路由器 R1 互连的三个子网 192.168.1.0/24、192.168.2.0/24 和 192.168.3.0/24 组成，Internet 由路由器 R3 互连的三个子网 192.1.1.0/24、192.1.2.0/24 和 192.1.3.0/24 组成。从 R1 和 R3 路由表可以看出，R1 路由表只包含用于指明通往内部网络各个子网的传输路径的路由项，其中网络地址 192.168.4.0/24 用于作为分配给连接在 Internet 上的终端的内部网络本地 IP 地址池。R3 路由表中只包含用于指明通往 Internet 各个子网的传输路径的路由项。终端

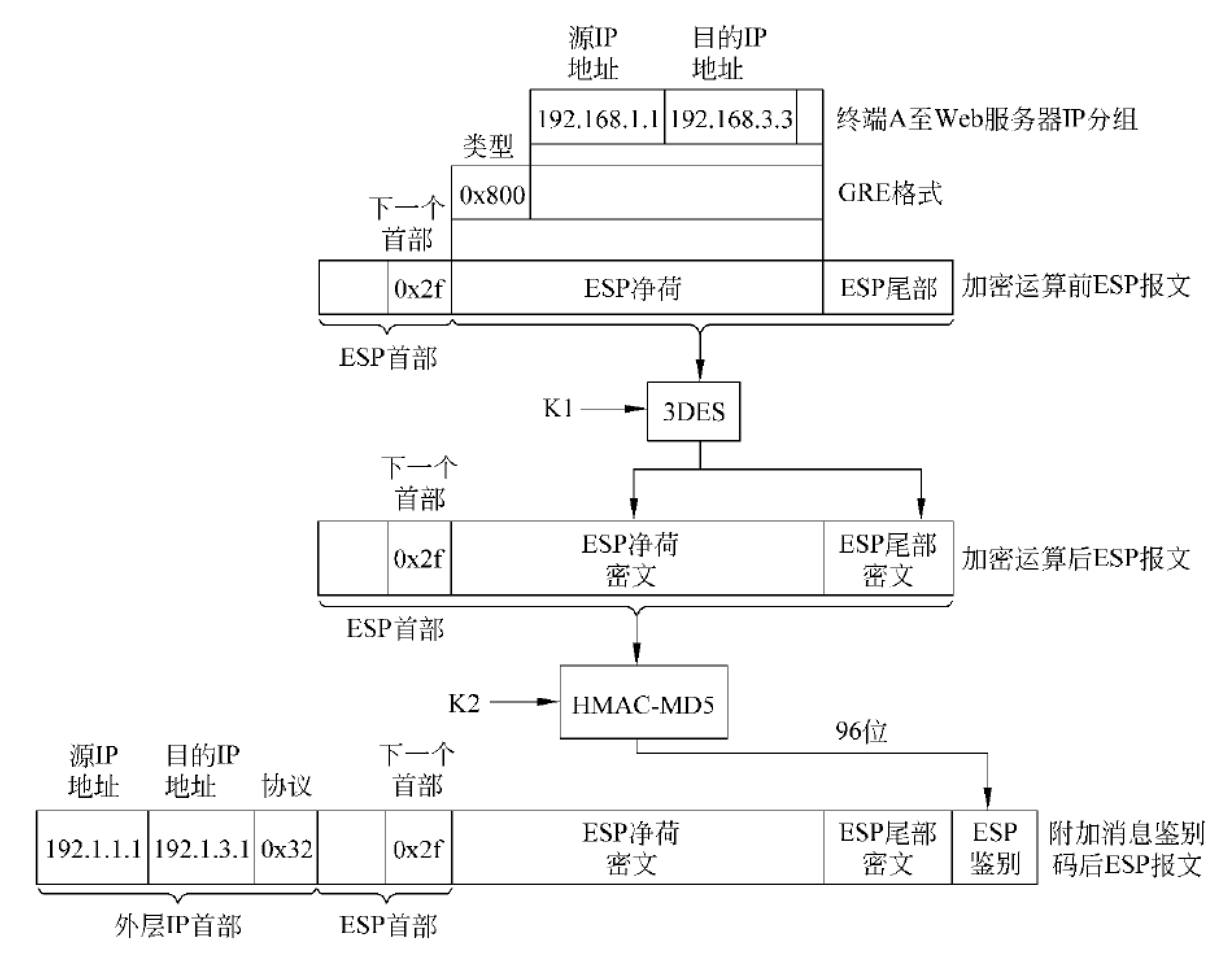


图 8.7 隧道 1 封装终端 A 至 Web 服务器 IP 分组过程

C 和终端 D 配置 Internet 全球 IP 地址，在实现远程接入前，无法访问内部网络资源，如内部网络的 Web 服务器。R2 一方面作为 VPN 服务器实现终端 C 和终端 D 的远程接入功能，另一方面实现内部网络和 Internet 互连。R1 和 R2 通过 RIP 建立用于指明通往内部网络各个子网的传输路径的路由项。R2 和 R3 通过 OSPF 建立用于指明通往 Internet 各个子网的传输路径的路由项。

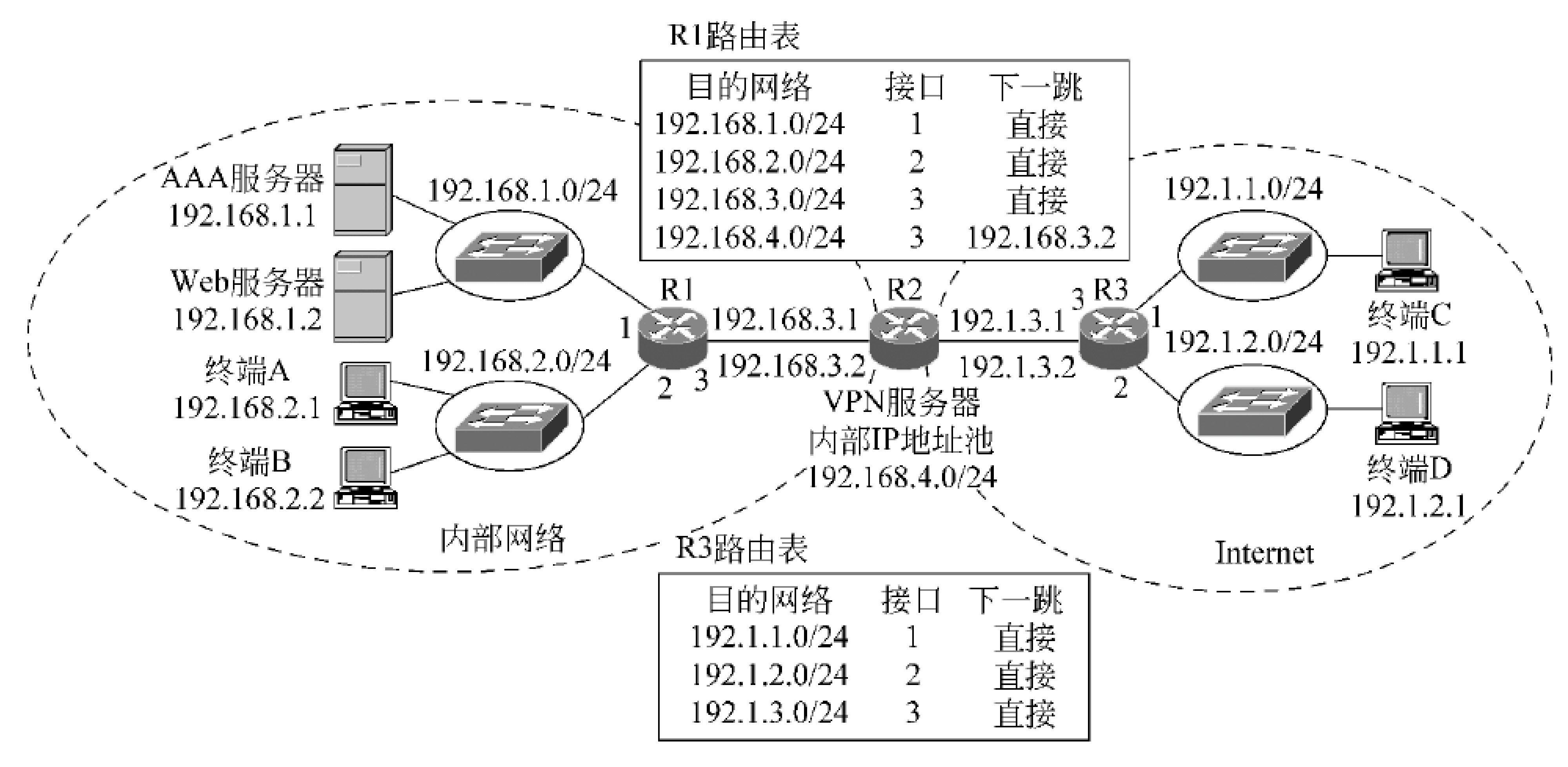


图 8.8 远程接入网络结构

Cisco Easy VPN 实现终端 C 和终端 D 远程接入过程如下：首先建立安全传输通道，然后鉴别远程接入用户身份，在完成用户身份鉴别后，向远程接入用户推送配置信息，包括本地 IP 地址、子网掩码等。最后建立 VPN 服务器 R2 与远程接入终端之间的 IP Sec 安全关联，用于实现数据远程接入终端与 VPN 服务器之间的安全传输。

2. Cisco Easy VPN 工作过程

(1) VPN 服务器需要配置的信息。

Cisco Easy VPN 的最大好处是简化远程终端的配置，只需将与安全传输有关的信息配置在 VPN 服务器上。VPN 服务器将远程终端分组，属于同一组的远程终端有着相同的共享密钥、本地 IP 地址和子网掩码等。除此之外，VPN 服务器还需配置建立 IP Sec 安全关联相关的 ISAKMP 策略(加密算法 256 位 AES、报文摘要算法 SHA、共享密钥鉴别方式和 DH-2)和变换集(ESP-3DES 和 ESP-SHA-HMAC)等。

(2) 建立远程终端与 VPN 服务器之间的 IP Sec 安全关联过程。

如图 8.9 所示，分三步完成远程终端与 VPN 服务器之间 IP Sec 安全关联的建立过程。第一步是建立安全传输通道，其目的是协商两端使用的加密算法、报文摘要算法、DH 组号和身份鉴别方式。Cisco Easy VPN 为了方便起见，约定双方使用 DH-2。图 8.8 中的终端 C 只需配置所属组的组标识符、共享密钥、VPN 服务器的 IP 地址与标识用户身份的用户名和口令。当终端 C 发起安全传输通道建立过程时，只需提供组标识符、用于生成密钥的参数 YC1 和用于表示采用 VPN 配置的 ISAKMP 策略的任意算法匹配符(图中用 * 表示)。VPN 服务器根据组标识符确定终端所属的组，获取共享密钥，选择优先级最高的 ISAKMP 策略作为和终端 C 约定的算法，将算法和用于生成密钥的参数 YR21 传输给终端 C，并通过鉴别信息 $AUTH_{R2}$($AUTH_{R2}=E_{PSK}$(SHA(3DES、SHA、YR21)))证明发送端身份。终端 C 通过发送鉴别信息一是证明发送端身份，二是让 VPN 服务器验证双方交换数据的完整性。

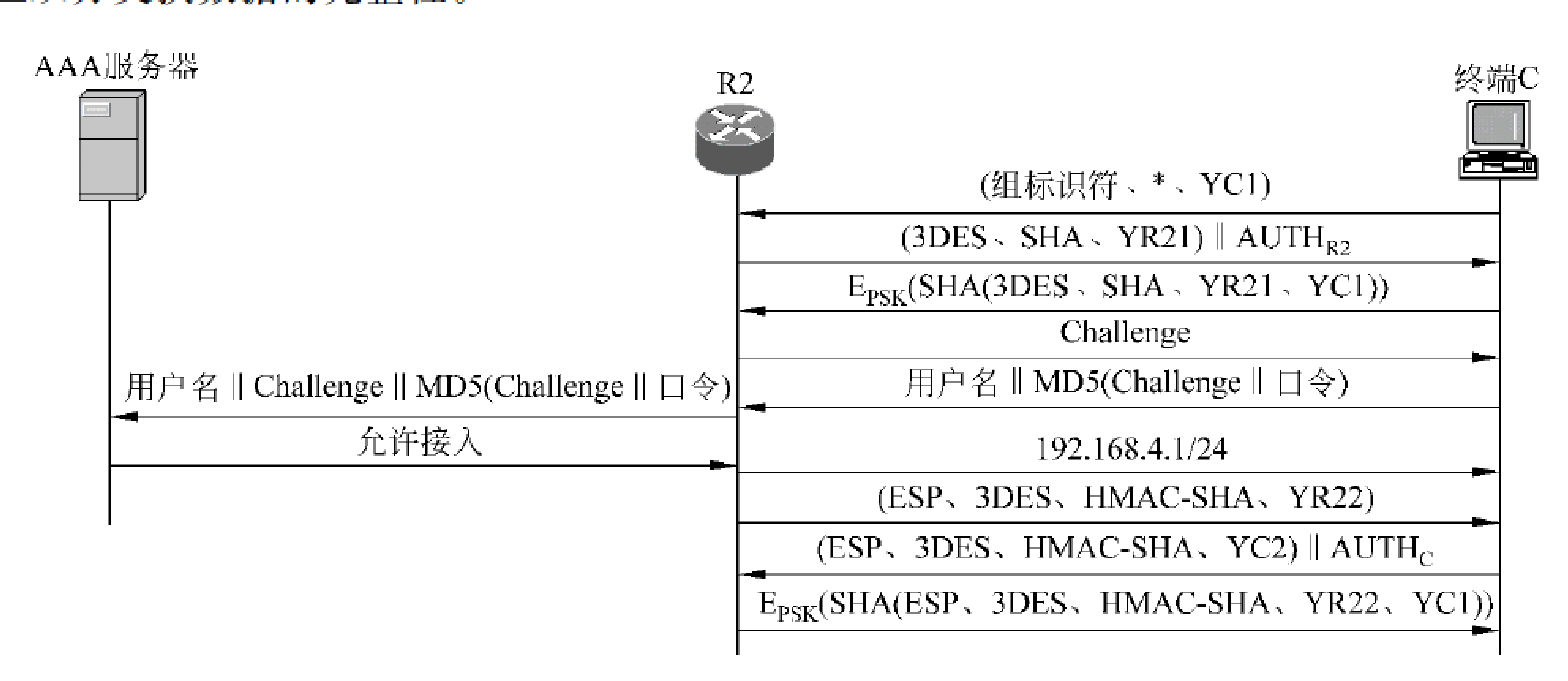


图 8.9 建立远程终端与 VPN 服务器之间的安全关联过程

建立安全传输通道后，由 VPN 服务器发起身份鉴别过程，VPN 服务器采用 CHAP 鉴别机制鉴别远程接入用户身份，因此，首先向终端 C 发送随机数 Challenge，终端 C 计算出 MD5(Challenge ‖ 口令)，并将用户名和计算结果发送给 VPN 服务器，VPN 服务器

将 Challenge、终端 C 发送的用户名和计算结果一起转发给鉴别服务器(AAA 服务器),由 AAA 服务器根据配置的授权用户标识信息验证远程接入用户身份,一旦证明是授权用户,向 VPN 服务器发送允许接入消息。VPN 服务器向终端 C 推送为终端 C 所属组配置的网络信息,如内部网络本地 IP 地址和子网掩码等。VPN 服务器和终端 C 之间可以采用建立安全传输通道时约定的加密算法、报文摘要算法和生成的密钥对身份鉴别过程和网络信息推送过程传输的数据进行加密和完整性检测。

完成身份鉴别过程后,VPN 服务器发起 IP Sec 安全关联建立过程。双方约定安全协议 ESP、加密算法 3DES 和 HMAC 算法 HMAC-SHA。

3. ESP 报文封装过程

终端 C 成功建立与 VPN 服务器之间的 IP Sec 安全关联后,可以访问内部网络 Web 服务器,终端 C 访问内部网络时使用 VPN 服务器推送给它的内部网络本地 IP 地址。终端 C 发送给内部网络 Web 服务器的 TCP 报文被封装成以终端 C 内部网络本地 IP 地址 192.168.4.1 为源 IP 地址、Web 服务器内部网络本地 IP 地址 192.168.1.2 为目的 IP 地址的 IP 分组,该 IP 分组称为内层 IP 分组。内层 IP 分组实现终端 C 至 VPN 服务器传输时,被封装成 ESP 报文,ESP 报文首部中下一个首部字段值 4 表明 ESP 报文净荷为内层 IP 分组。完成加密和消息鉴别码运算的 ESP 报文被封装成 UDP 报文,两端用端口号 4500 表明 UDP 报文净荷是 ESP 报文。UDP 报文被封装成源和目的 IP 地址为终端 C 和 VPN 服务器全球 IP 地址 192.1.1.1 和 192.1.3.1 的外层 IP 分组,整个封装过程如图 8.10 所示。外层 IP 分组经过终端 C 与 VPN 服务器之间的 Internet 到达 VPN 服务器,由 VPN 服务器分离出内层 IP 分组,并经过 VPN 连接的内部网络实现内层 IP 分组 VPN 服务器至 Web 服务器的传输过程。

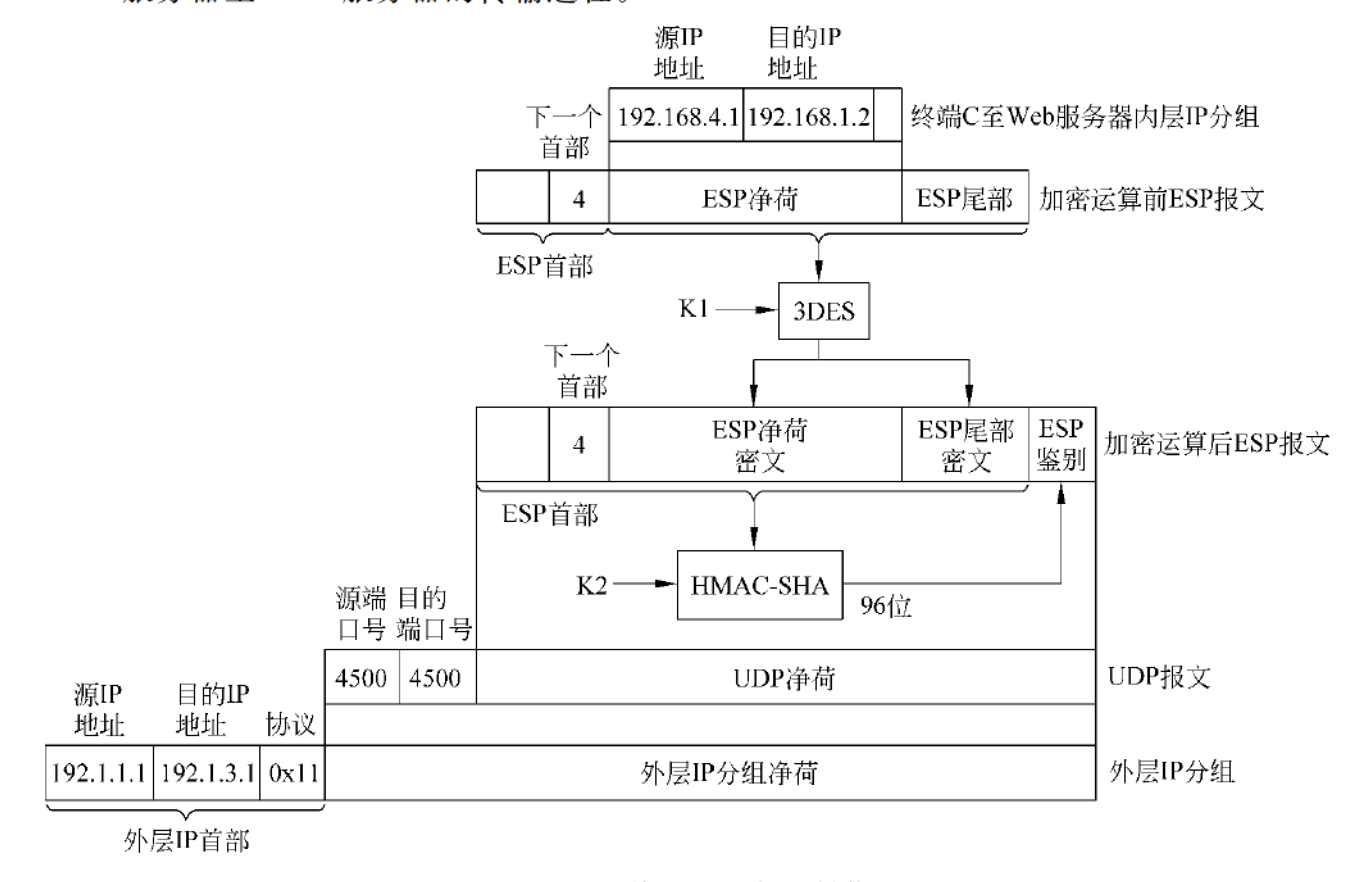


图 8.10　远程接入 ESP 报文封装过程

8.2 例题解析

8.2.1 自测题

1. 选择题

(1) 下述________不是专用网络的特点。

A. 使用本地 IP 地址　　B. 不和其他网络共享传输路径
C. 不能和其他网络相互通信　　D. 使用 TCP/IP 协议栈

(2) 下述________是专用网络和虚拟专用网络的本质区别。

A. 使用本地 IP 地址
B. 实现数据内部网络子网间安全传输
C. 使用公共网络提供的数据传输通路
D. 使用 TCP/IP 协议栈

(3) 下述________不是隧道的功能。

A. 实现内部网络各个子网间互连
B. 实现连接在 Internet 上的终端远程接入内部网络
C. 两个 IPv6 网络通过 IPv4 网络实现互连
D. 实现内部网络终端和公共网络终端之间的通信

(4) 下述________不是虚拟专用网络需要解决的问题。

A. 使用本地 IP 地址的 IP 分组如何经过 Internet 传输的问题
B. 如何保证数据经过 Internet 安全传输的问题
C. 如何防止其他网络冒充内部网络子网的问题
D. 如何实现内部网络终端和公共网络终端之间通信的问题

(5) 下述________不是 IP Sec 提供的功能。

A. 实现使用本地 IP 地址的 IP 分组经过 Internet 传输
B. 实现数据经过 Internet 的安全传输
C. 实现数据的源端鉴别
D. 实现源端和目的端之间的相互身份鉴别

(6) 下述________不是定期重建 IP Sec 安全关联的好处。

A. 定期更换加密密钥和 HAMC 密钥
B. 定期重新鉴别两端身份
C. 定期更换加密算法和 HMAC 算法
D. 定期初始化两端参数,如 SPI 和序号

(7) 下述________不是虚拟专用网络的好处。

A. 通过 Internet 实现内部网络各个子网间互连
B. 实现数据内部网络子网间的安全传输
C. 内部网络独立分配 IP 地址空间

D. 通过 NAT 解决本地 IP 地址与全球 IP 地址之间转换

(8) IP Sec 不能实现________数据安全传输。

A. 链路层　　B. 网络层　　C. 传输层　　D. 应用层

(9) 关于隧道，下述________是错误的。

A. 隧道两端是分配 IP 地址的两个接口

B. 允许多种不同封装格式的分组从隧道一端传输到隧道另一端

C. 经过隧道传输的分组对隧道两端之间的 IP 分组传输路径是透明的

D. 经过隧道传输的必须是传输层以上的 PDU

(10) 下述________和 VPN 接入无关。

A. 远程终端分配内部网络本地 IP 地址

B. 连接 Internet 的远程终端访问内部网络中的资源

C. 建立远程终端与内部网络连接 Internet 的路由器之间的安全隧道

D. 远程终端拨号接入方式接入 Internet

2. 填空题

(1) 目前的 VPN 通常由________实现内部网络各个子网间互连，内部网络分配独立的 IP 地址空间，解决内部网络终端间 IP 分组传输的关键是________，它实现以内部网络本地 IP 地址为源和目的 IP 地址的 IP 分组经过 Internet 的传输过程。

(2) VPN 和 IP Sec 结合的主要原因是隧道的传输路径是________，经过隧道传输的分组作为________，IP Sec 能够实现 IP 分组净荷的安全传输。

(3) IP Sec 安全协议分为________和________，________能够实现 IP 分组的源端鉴别和完整性检测，________能够实现 IP 分组净荷的加密传输。________采用的加密算法主要有________、________和________。IP Sec 采用 HMAC 解决源端鉴别和完整性检测，常用的两种 HMAC 算法是________和________。

(4) 隧道两端是________，实现分组经过隧道传输的前提是________，经过隧道传输的分组必须作为以________为源和目的 IP 地址的 IP 分组的净荷。

(5) IP Sec 实现 IP 分组安全传输的前提是建立 IP Sec 安全关联，建立 IP Sec 安全关联的方式有________和________，其中________需要使用 ISAKMP。ISAKMP 建立 IP Sec 安全关联过程分为________，其中，________主要约定安全传输通道使用的________、________、________和________，________主要约定 IP Sec 安全关联使用的________和________。如果约定的安全协议是________，还需约定________。

(6) IP-in-IP 要求外层 IP 分组的净荷只能是________，GRE 允许外层 IP 分组的净荷可以是________，因为 GRE 能够________。

(7) VPN 中内部网络各个子网分配的 IP 地址________，VPN 中的边缘路由器实现________和________互连，其中连接________的接口往往是隧道的源端。边缘路由器路由表既要包含________，又要包含________。

3. 名词解释

____ DH 组号　　____隧道
____ IP 隧道　　____ IP Sec 安全关联
____ IP Sec　　____ ESP
____远程接入　　____ VPN
____ L2TP　　____第二层隧道
____ AH　　____ ISAKMP
____专用网络　　____ Diffie-Hellman 密钥交换协议

(a) 用于在 IP 层实现数据安全传输的协议系列。

(b) 封装安全净荷，属于 IP Sec 的一种安全协议，用于实现经过 IP 层传输的数据的保密性和完整性。

(c) 鉴别首部，属于 IP Sec 的一种安全协议，用于实现经过 IP 层传输的数据的完整性。

(d) Internet 安全关联和密钥管理协议，一种用于创建 IP Sec 安全关联和实现密钥分配的标准通用框架。

(e) 一个采用 Diffie-Hellman 密钥交换协议产生密钥时，用来选择原根和素数位数的编号，编号越大，素数位数越多，密钥的安全性越好。

(f) 一种通过将任意格式分组作为以两端 IP 地址为源和目的 IP 地址的 IP 分组净荷，实现该分组经过两端之间 IP 分组传输路径传输的技术。通常情况下，两端之间的 IP 分组传输路径经过公共网络，如 Internet。

(g) 一种通过隧道将连接公共网络上，并分配全球 IP 地址的终端接入内部网络，分配内部网络本地 IP 地址，并以内部网络本地 IP 地址访问内部网络资源的技术。

(h) 一种通过两端之间传输路径经过公共网络的隧道实现内部网络各个子网互连，并使数据经过隧道传输时具有经过专用物理链路传输时相同的安全性的内部网络结构。

(i) 第二层隧道协议，一种用于创建传输链路层帧的隧道的协议。隧道两端之间的 IP 分组传输路径经过公共网络，如 Internet。

(j) 一种用于传输链路层帧的隧道，隧道两端之间的 IP 分组传输路径经过公共网络，如 Internet。

(k) 一种用于传输 IP 分组的隧道，隧道两端之间的 IP 分组传输路径经过公共网络，如 Internet。经过隧道传输的 IP 分组称为内层 IP 分组，以隧道两端 IP 地址为源和目的 IP 地址的 IP 分组称为外层 IP 分组。

(l) 一种为在 IP 层实现数据安全传输而建立的单向连接，其目的是约定连接两端使用的安全协议、加密和 HMAC 算法、加密和 HMAC 密钥等。

(m) 一种有着独立的 IP 地址空间、独立的资源，用专用物理链路实现子网间互连，不和其他网络共享任何资源的内部网络结构。

(n) 一种在约定原根和素数的前提下，通过交换数据创建对称密钥的协议。该协议在原根和素数公开，交换的数据公开的情况下，仍能保证对称密钥的保密性。

4. 判断题

(1) 由于隧道格式是以隧道两端 IP 地址为源和目的 IP 地址的 IP 分组，因此隧道格式的净荷只能是传输层以上的 PDU。

(2) VPN 中内部网络各个子网的 IP 地址空间是相互独立的，允许两个不同子网分配相同的本地 IP 地址空间。

(3) VPN 中连接在不同内部网络子网的终端可以通过本地 IP 地址实现相互通信。

(4) 隧道经过的 IP 分组传输路径对隧道格式中的净荷是透明的。

(5) VPN 中 IP Sec 的作用是实现数据经过隧道的安全传输。

(6) 建立 IP Sec 安全关联的目的是约定两端与实现数据安全传输相关的参数。

(7) ESP 实现 IP Sec 安全关联两端之间传输的数据的保密性和完整性。

(8) AH 实现 IP Sec 安全关联两端之间传输的数据的完整性。

(9) 配置 DH 组号的目的是需要通过 Diffie-Hellman 密钥交换协议生成加密和 HMAC 密钥。

(10) 由于隧道两端之间是经过公共网络的 IP 分组传输路径，因此内部网络各个子网间传输的 IP 分组需要通过 NAT 将本地 IP 地址转换成全球 IP 地址。

8.2.2　自测题答案

1. 选择题答案

(1) D，并不是只有专用网络使用 TCP/IP 协议栈。

(2) C，虚拟专用网络用隧道实现内部网络各个子网间互连，隧道两端之间的传输路径经过公共网络，且该内部网络不能独占隧道两端之间传输路径的带宽。

(3) D，VPN 的主要任务是用隧道实现内部网络各个子网间互连，并保证经过隧道传输的数据的保密性和完整性。

(4) D，VPN 的主要任务不是实现内部网络终端与公共网络终端之间的通信。

(5) A，该项功能由隧道实现，VPN 的技术基础是隧道和 IP Sec。

(6) C，定期重建的 IP Sec 安全关联往往采用相同的策略和变换集配置，因此不会改变加密和 HMAC 算法。

(7) D，VPN 的主要任务不是实现内部网络终端与公共网络终端之间的通信。

(8) A，IP Sec 实现 IP 分组净荷的安全传输，IP 分组净荷不应该是链路层帧。应用层数据封装成传输层 PDU 后，作为 IP 分组的净荷。

(9) D，链路层帧可以作为第二层隧道的净荷，因此 IP Sec 和隧道结合可以经过 IP 分组传输路径安全传输链路层帧。

(10) D，远程终端需要连接在 Internet 上，分配全球 IP 地址，但无需指定远程终端接入 Internet 的方式。

2. 填空题答案

(1) Internet，隧道。

(2) IP 分组传输路径，IP 分组的净荷。

(3) ESP，AH，AH，ESP，ESP，DES，3DES，AES，HAMC-MD5，HMAC-SHA。

(4) 分配全球 IP 地址的接口，公共网络建立隧道两端之间的 IP 分组传输路径，隧道两端全球 IP 地址。

(5) 静态配置，动态建立，动态建立，两个阶段，第一阶段，加密算法，报文摘要算法，DH 组号，身份鉴别方式，第二阶段，安全协议，HMAC 算法，ESP，加密算法。

(6) 内层 IP 分组，以太网类型字段值支持的数据类型，通过类型字段值给出 GRE 净荷类型。

(7) 不相同的，内部网络子网，公共网络，公共网络，用于指明通往内部网络其他子网传输路径的路由项，用于指明公共网络通往隧道另一端传输路径的路由项。

3. 名词解释答案

e	DH 组号	f	隧道
k	IP 隧道	l	IP Sec 安全关联
a	IP Sec	b	ESP
g	远程接入	h	VPN
i	L2TP	j	第二层隧道
c	AH	d	ISAKMP
m	专用网络	n	Diffie-Hellman 密钥交换协议

4. 判断题答案

(1) 错，隧道格式净荷可以是多种格式的分组，包括链路层帧。

(2) 错，VPN 中各个内部网络子网是内部网络的有机组成部分，必须分配不同的本地 IP 地址。

(3) 对，这是 VPN 的特征。

(4) 对，对于隧道格式中的净荷，隧道等同于点对点物理链路，隧道经过的传输路径对其是透明的。

(5) 对，隧道两端之间传输路径是 IP 分组传输路径，因此用 IP Sec 实现隧道两端之间的安全传输。

(6) 对，IP Sec 安全关联建立过程就是两端协商与实现数据安全传输相关的参数的过程。

(7) 对，ESP 具有加密和完整性检测功能。

(8) 对，AH 没有加密功能。

(9) 对，两端通过选择 DH 组号确定两端使用的原根和素数。

(10) 错，经过隧道传输时，整个以内部网络本地 IP 地址为源和目的 IP 地址的内层 IP 分组作为以隧道两端全球 IP 地址为源和目的 IP 地址的外层 IP 分组的净荷。

8.2.3 简答题解析

1. 简述隧道和 IP Sec 是实现 VPN 的基础的理由。

回答：隧道是一种通过公共网络传输任意格式分组的技术，它将任意格式分组封装后作为以隧道两端 IP 地址为源和目的 IP 地址的外层 IP 分组的净荷，在完成外层 IP 分组隧道两端之间传输的同时，实现任意格式分组隧道一端至隧道另一端的传输过程。IP

Sec 能够实现 IP 分组净荷隧道两端之间的安全传输。隧道与 IP Sec 结合可以实现任意格式分组公共网络任意两个端点之间的安全传输。这恰恰是 VPN 的设计目标，用公共网络实现内部网络各个子网之间互连，同时又能保证内部网络封装形式的数据各个子网间的安全传输。

2. 简述 VPN 和 NAT 的区别和联系。

回答：VPN 的设计目标是用公共网络实现内部网络各个子网之间互连，同时又能保证内部网络封装形式的数据各个子网间的安全传输。因此，VPN 主要用于实现内部网络各个子网间的安全通信。NAT 主要用于实现内部网络终端与公共网络终端之间的通信。在只需要实现内部网络终端之间通信的 VPN 中，公共网络对于内部网络终端是透明的，VPN 不需要 NAT 技术，但如果某个 VPN 既要实现内部网络终端之间通信，又要实现内部网络终端与公共网络终端之间通信，需要在隧道和 IP Sec 的技术上增加 NAT 技术。

3. 简述 Cisco Easy VPN 与点对点隧道和 IP Sec 的区别。

回答：一是点对点隧道两端需要配置匹配的 ISAKMP 策略和 IP Sec 变换集，但 Cisco Easy VPN 往往只需在 VPN 服务器上配置 ISAKMP 策略和 IP Sec 变换集，在建立 IP Sec 安全关联过程中由 VPN 服务器将 ISAKMP 策略和 IP Sec 变换集推送给远程终端。二是 Cisco Easy VPN 需要以组为单位组织远程终端，属于同一组的远程终端使用相同的共享密钥和内部网络配置信息，但可以具有不同的标识信息。三是 Cisco Easy VPN 需要创建动态加密映射，允许任何 IP Sec 安全关联发起者成为该动态加密映射的另一端。四是 VPN 服务器在成功建立安全传输通道后，需要鉴别远程终端身份，并在成功鉴别远程终端身份后，向远程终端推送内部网络配置信息，如内部网络本地 IP 地址和子网掩码等。五是点对点隧道在创建隧道时，通过在隧道两端静态配置内部网络本地 IP 地址和路由协议，动态建立用于指明通往内部网络各个子网的传输路径的路由项。但 Cisco Easy VPN 不需要静态配置 VPN 服务器与远程终端之间的隧道，在成功建立与某个远程终端之间的 IP Sec 安全关联后，动态创建 VPN 服务器与远程终端之间的隧道，并建立用于指明内部网络内通往该远程终端的传输路径的路由项。

8.3 实　　验

8.3.1 点对点 IP 隧道配置实验

1. 实验内容

(1) 完成虚拟专用网络设计。

(2) 完成点对点 IP 隧道配置。

(3) 验证内部网络路由项建立过程。

(4) 验证公共网络隧道两端之间传输路径建立过程。

2. 网络结构

网络结构采用图 8.1 所示的虚拟专用网络结构。首先建立图 8.2 所示的隧道 0 和隧

道1,通过OSPF在公共网络各个路由器(包括边缘路由器R1、R2和R3)中建立用于指明隧道两端之间传输路径的路由项。对应图8.2所示的内部网络逻辑结构,通过RIP在边缘路由器R1、R2和R3中创建如图所示的用于指明通往内部网络中各个子网的传输路径的路由项。因此,边缘路由器中既要配置OSPF进程,用于建立隧道两端经过公共网络的传输路径,又要配置RIP进程,用于建立通往其他边缘路由器连接的内部网络子网的传输路径。

3. 实验步骤

(1) 启动Packet Tracer,在逻辑工作区根据图8.1所示的网络结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图8.11所示。

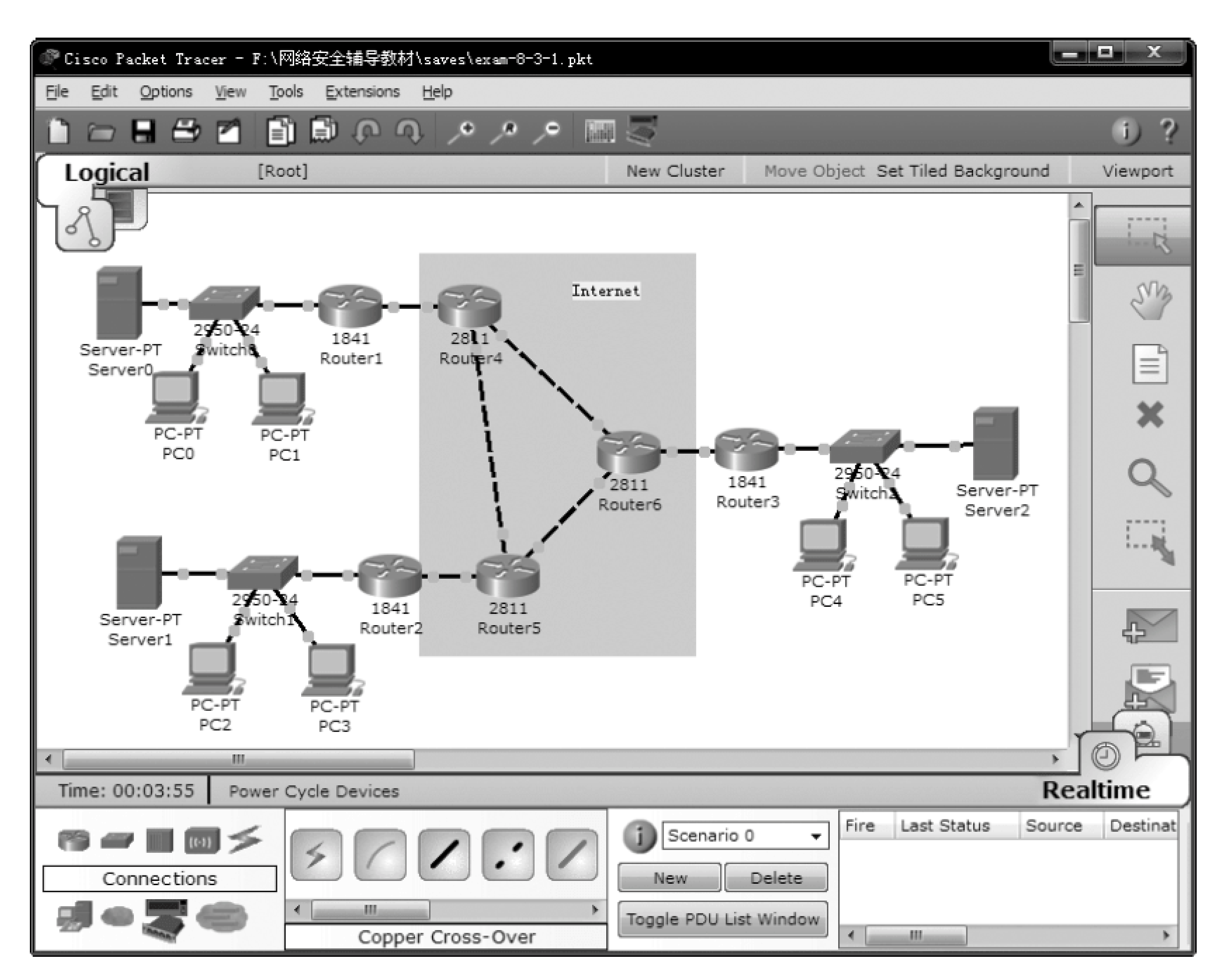


图8.11 放置和连接设备后的逻辑工作区界面

(2) 根据图8.1所示的配置信息完成各个路由器(Router1～Router6)接口的IP地址和子网掩码配置,将属于公共网络的路由器接口配置成OSPF区域1接口,这些接口包括路由器Router4～Router6的全部接口和路由器Router1～Router3连接公共网络的接口。完成OSPF配置后,公共网络中各个路由器(包括边缘路由器R1、R2和R3)建立通往公共网络中各个子网的传输路径。可以通过这些路由器中类型为O的路由项,建立边缘路由器Router1全球IP地址为192.1.1.1的接口与边缘路由器Router2全球IP地址为192.1.2.1的接口之间的传输路径,建立边缘路由器Router1全球IP地址为192.1.1.1的接口与边缘路由器Router3全球IP地址为192.1.3.1的接口之间的传输路径,建立这两对接口之间的传输路径是保证图8.2中隧道0和隧道1两端之间连通性的前提。路由器Router1～Router6的完整路由表如图8.12～图8.17所示。需要指出的是,路由器

Router4～Router6 路由表中没有用于指明通往内部网络各个子网的传输路径的路由项，内部网络对这些路由器是透明的。

Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
C	192.168.5.0/24	Tunnel1	---	0/0
C	192.1.1.0/24	FastEthernet0/1	---	0/0
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.4.0/24	Tunnel0	---	0/0
O	192.1.2.0/24	FastEthernet0/1	192.1.1.2	110/3
O	192.1.3.0/24	FastEthernet0/1	192.1.1.2	110/3
O	192.1.4.0/24	FastEthernet0/1	192.1.1.2	110/2
O	192.1.5.0/24	FastEthernet0/1	192.1.1.2	110/3
O	192.1.6.0/24	FastEthernet0/1	192.1.1.2	110/2
R	192.168.2.0/24	Tunnel0	192.168.4.2	120/1
R	192.168.3.0/24	Tunnel1	192.168.5.2	120/1

图 8.12　边缘路由器 Router1 完整路由表

Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet0/1	---	0/0
C	192.168.2.0/24	FastEthernet0/0	---	0/0
C	192.168.4.0/24	Tunnel0	---	0/0
O	192.1.1.0/24	FastEthernet0/1	192.1.2.2	110/3
O	192.1.3.0/24	FastEthernet0/1	192.1.2.2	110/3
O	192.1.4.0/24	FastEthernet0/1	192.1.2.2	110/2
O	192.1.5.0/24	FastEthernet0/1	192.1.2.2	110/2
O	192.1.6.0/24	FastEthernet0/1	192.1.2.2	110/3
R	192.168.5.0/24	Tunnel0	192.168.4.1	120/1
R	192.168.1.0/24	Tunnel0	192.168.4.1	120/1
R	192.168.3.0/24	Tunnel0	192.168.4.1	120/2

图 8.13　边缘路由器 Router2 完整路由表

Routing Table for Router3

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	FastEthernet0/1	---	0/0
C	192.168.3.0/24	FastEthernet0/0	---	0/0
C	192.168.5.0/24	Tunnel1	---	0/0
O	192.1.1.0/24	FastEthernet0/1	192.1.3.2	110/3
O	192.1.2.0/24	FastEthernet0/1	192.1.3.2	110/3
O	192.1.4.0/24	FastEthernet0/1	192.1.3.2	110/3
O	192.1.5.0/24	FastEthernet0/1	192.1.3.2	110/2
O	192.1.6.0/24	FastEthernet0/1	192.1.3.2	110/2
R	192.168.1.0/24	Tunnel1	192.168.5.1	120/1
R	192.168.2.0/24	Tunnel1	192.168.5.1	120/2
R	192.168.4.0/24	Tunnel1	192.168.5.1	120/1

图 8.14　边缘路由器 Router3 完整路由表

Routing Table for Router4

Type	Network	Port	Next Hop IP	Metric
C	192.1.1.0/24	FastEthernet0/0	---	0/0
C	192.1.4.0/24	FastEthernet0/1	---	0/0
C	192.1.6.0/24	FastEthernet1/0	---	0/0
O	192.1.2.0/24	FastEthernet0/1	192.1.4.2	110/2
O	192.1.3.0/24	FastEthernet1/0	192.1.6.2	110/2
O	192.1.5.0/24	FastEthernet0/1	192.1.4.2	110/2
O	192.1.5.0/24	FastEthernet1/0	192.1.6.2	110/2

图 8.15　公共网络 Router4 完整路由表

Routing Table for Router5

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet0/0	---	0/0
C	192.1.4.0/24	FastEthernet0/1	---	0/0
C	192.1.5.0/24	FastEthernet1/0	---	0/0
O	192.1.1.0/24	FastEthernet0/1	192.1.4.1	110/2
O	192.1.3.0/24	FastEthernet1/0	192.1.5.2	110/2
O	192.1.6.0/24	FastEthernet0/1	192.1.4.1	110/2
O	192.1.6.0/24	FastEthernet1/0	192.1.5.2	110/2

图 8.16　公共网络 Router5 完整路由表

Routing Table for Router6

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	FastEthernet0/0	---	0/0
C	192.1.5.0/24	FastEthernet1/0	---	0/0
C	192.1.6.0/24	FastEthernet0/1	---	0/0
O	192.1.1.0/24	FastEthernet0/1	192.1.6.1	110/2
O	192.1.2.0/24	FastEthernet1/0	192.1.5.1	110/2
O	192.1.4.0/24	FastEthernet0/1	192.1.6.1	110/2
O	192.1.4.0/24	FastEthernet1/0	192.1.5.1	110/2

图 8.17　公共网络 Router6 完整路由表

(3) 在路由器 Router1 中配置隧道 0(Tunnel 0)和隧道 1(Tunnel 1)两端信息。一端是 Router1 连接公共网络接口 FastEthernet0/0,另一端通过全球 IP 地址指定,隧道 0 的另一端是全球 IP 地址 192.1.2.1,隧道 1 的另一端是全球 IP 地址 192.1.3.1。可以为隧道配置本地 IP 地址,Router1 分别为隧道 0 和隧道 1 配置本地 IP 地址 192.168.4.1 和 192.168.5.1。在 Router2 中配置隧道 0(Tunnel 0)两端信息,在 Router3 中配置隧道 1(Tunnel 1)两端信息。完成上述配置后,Router1～Router3 中路由表中出现目的网络为接口直接连接的和隧道直接连接的内部网络子网的路由项。

(4) 在 Router1～Router3 中配置 RIP 进程,给出参与建立动态路由项的直接连接的内部网络子网(包括接口直接连接的和隧道直接连接的内部网络子网),如 Router1 配置的内部网络子网 192.168.1.0/24(接口直接连接的内部网络子网)和 192.168.4.0/24 与 192.168.5.0/24(隧道直接连接的内部网络子网),完成 Router1～Router3 RIP 进程配置后,Router1～Router3 路由表中出现类型为 R、用于指明内部网络各个子网的传输路径的路由项。Router1～Router3 路由表如图 8.12～图 8.14 所示。

(5) 各个路由器建立完整路由表后,可以分析两层 IP 分组传输路径,一是公共网络中目的网络为全球 IP 地址的路由项,其中最重要的是用于建立隧道 0 和隧道 1 两端之间传输路径的路由项。二是建立内部网络各个子网之间传输路径的路由项,这些路由项只存在于边缘路由器,公共网络隐身为点对点 IP 隧道。

(6) 发起 PC0 访问 Server2 的过程,PC0 成功访问 Server2 的界面如图 8.18 所示。TCP 报文的传输路径分为三段:一是 PC0 至边缘路由器 Router1 的传输路径,TCP 报文被封装成 IP 分组,协议字段值 6 表明了 IP 分组的净荷是 TCP 报文,IP 分组的源和目的 IP 地址分别是 PC0 和 Server2 的本地 IP 地址 192.168.1.1 和 192.168.3.3,IP 分组格式如图 8.19 所示。二是隧道 1 两端之间的传输路径,即边缘路由器 Router1 连接公共网络接口至边缘路由器 Router3 连接公共网络接口之间的 IP 分组传输路径,内层 IP 分组被

封装成隧道格式，封装过程如图 8.20 所示。GRE 格式中通过类型字段值 0x800 表明了 GRE 格式净荷是内层 IP 分组。外层 IP 分组的协议字段值 0x2f(十进制值 47)表明外层 IP 分组净荷是 GRE 格式。三是边缘路由器 Router3 至 Server2 的传输路径，IP 分组格式与图 8.19 所示相同。

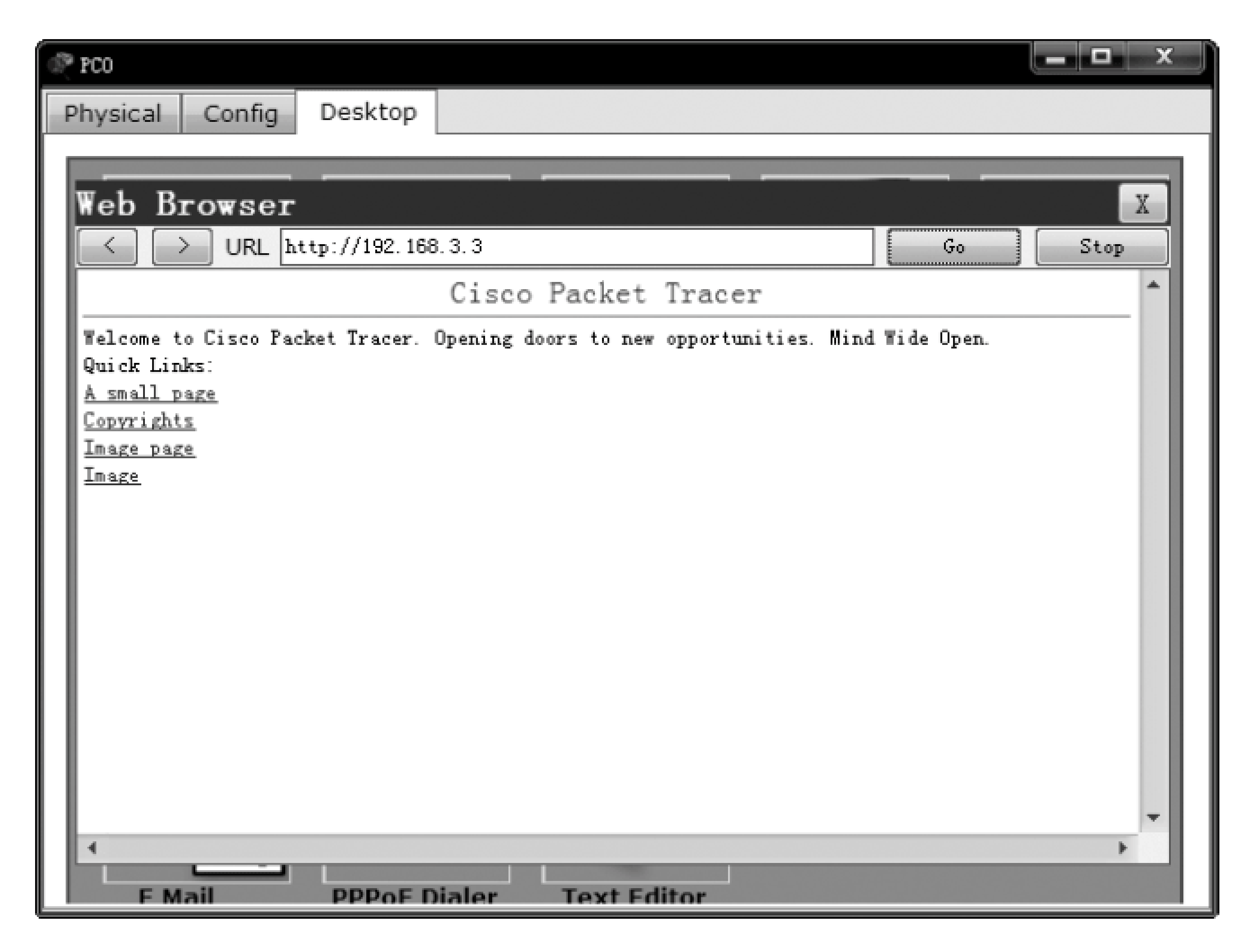


图 8.18　PC0 成功访问 Web Server 界面

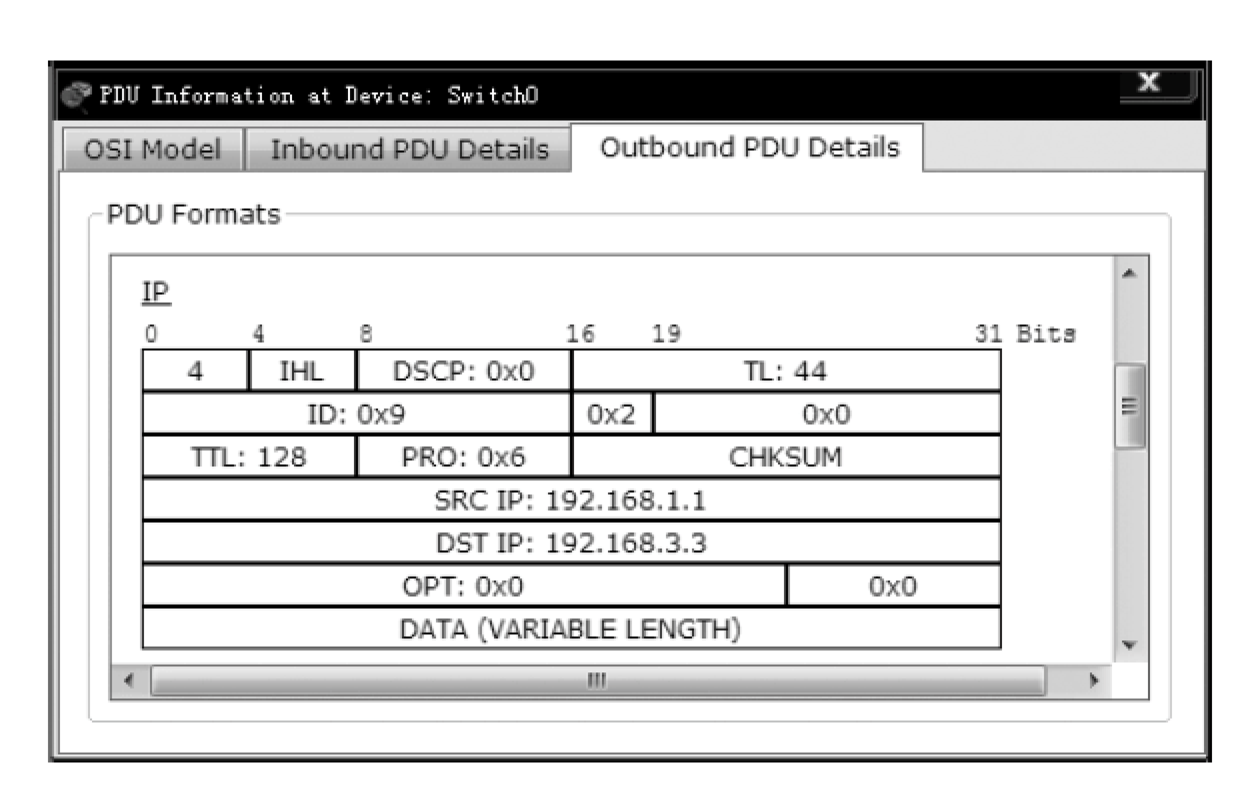


图 8.19　PC0 创建的内层 IP 分组格式

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
```

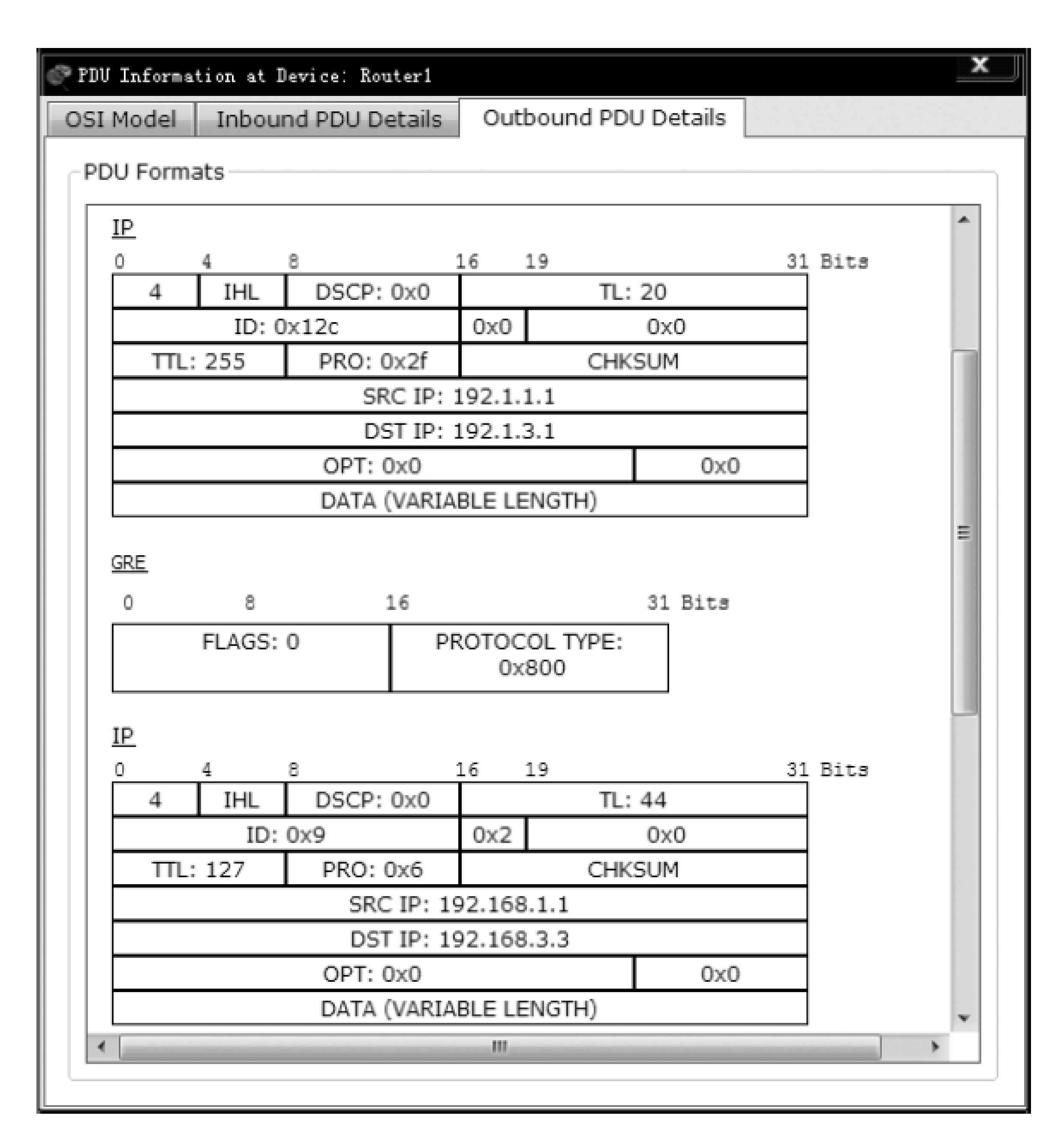


图 8.20　经过隧道 1 传输的外层 IP 分组格式

```
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface tunnel 0      (定义隧道 0,并开始隧道 0 配置过程)
Router(config-if)#ip address 192.168.4.1 255.255.255.0      (为隧道 0 定义本地 IP 地址)
Router(config-if)#tunnel source FastEthernet0/1
                        (指定隧道 0 的源端是连接公共网络接口 FastEthernet0/1)
Router(config-if)#tunnel destination 192.1.2.1
                        (指定隧道 0 的目的端是全球 IP 地址为 192.1.2.1 的接口)
Router(config-if)#exit
Router(config)#interface tunnel 1      (定义隧道 1,并开始隧道 1 配置过程)
Router(config-if)#ip address 192.168.5.1 255.255.255.0      (为隧道 1 定义本地 IP 地址)
Router(config-if)#tunnel source FastEthernet0/1
                        (指定隧道 1 的源端是连接公共网络接口 FastEthernet0/1)
Router(config-if)#tunnel destination 192.1.3.1
                        (指定隧道 1 的目的端是全球 IP 地址为 192.1.3.1 的接口)
Router(config-if)#exit
Router(config)#router rip      (启动用于建立通往内部网络各个子网的传输路径的 RIP 进程)
Router(config-router)#network 192.168.1.0      (配置 Router1 接口直接连接的内部网络子网)
Router(config-router)#network 192.168.4.0      (配置 Router1 隧道 0 直接连接的内部网络子网)
Router(config-router)#network 192.168.5.0      (配置 Router1 隧道 1 直接连接的内部网络子网)
Router(config-router)#exit
Router(config)#router ospf 11      (启动用于建立通往公共网络各个子网的传输路径的 OSPF 进程)
```

Router(config-router)#network 192.1.1.0 0.0.0.255 area 1

(将接口 IP 地址属于 CIDR 地址块 192.1.1.0/24 的路由器接口分配给区域 1。0.0.0.255 是子网掩码 255.255.255.0 的反码,指定直接连接公共网络的接口参与 OSPF 动态路由项的建立过程)

Router(config-router)#exit

(2) Router2 命令行配置过程。

Router>enable

Router#configure terminal

Router(config)#interface FastEthernet0/0

Router(config-if)#no shutdown

Router(config-if)#ip address 192.168.2.254 255.255.255.0

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

Router(config-if)#no shutdown

Router(config-if)#ip address 192.1.2.1 255.255.255.0

Router(config-if)#exit

Router(config)#interface tunnel 0　　(定义隧道 0,并开始隧道 0 配置过程)

Router(config-if)#ip address 192.168.4.2 255.255.255.0

(配置和隧道 0 另一端具有相同网络地址的本地 IP 地址)

Router(config-if)#tunnel source FastEthernet0/1

(指定隧道 0 的源端是连接公共网络接口 FastEthernet0/1,它的全球 IP 地址必须是 192.1.2.1)

Router(config-if)#tunnel destination 192.1.1.1

(指定隧道 0 的目的端是全球 IP 地址为 192.1.1.1 的接口。该接口必须是 Router1 连接公共网络接口 FastEthernet0/1)

Router(config-if)#exit

Router(config)#router rip

Router(config-router)#network 192.168.2.0

Router(config-router)#network 192.168.4.0

Router(config-router)#exit

Router(config)#router ospf 22

Router(config-router)#network 192.1.2.0 0.0.0.255 area 1

(指定直接连接公共网络的接口参与 OSPF 动态路由项的建立过程)

Router(config-router)#exit

(3) Router3 命令行配置过程。

Router>enable

Router#configure terminal

Router(config)#interface FastEthernet0/0

Router(config-if)#no shutdown

Router(config-if)#ip address 192.168.3.254 255.255.255.0

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

```
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface tunnel 1     (定义隧道 1,并开始隧道 1 配置过程)
Router(config-if)#ip address 192.168.5.2 255.255.255.0
                              (配置和隧道 1 另一端具有相同网络地址的本地 IP 地址)
Router(config-if)#tunnel source FastEthernet0/1
     (指定隧道 1 的源端是连接公共网络接口 FastEthernet0/1,它的全球 IP 地址必须是 192.
     1.3.1)
Router(config-if)#tunnel destination 192.1.1.1
     (指定隧道 1 的目的端是全球 IP 地址为 192.1.1.1 的接口。该接口必须是 Router1 连接
     公共网络接口 FastEthernet0/1)
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.5.0
Router(config-router)#exit
Router(config)#router ospf 33
Router(config-router)#network 192.1.3.0 0.0.0.255 area 1
                              (指定直接连接公共网络的接口参与 OSPF 动态路由项的建立过程)
Router(config-router)#exit
```

(4) Router4 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.6.1 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 44
Router(config-router)#network 192.1.1.0 0.0.0.255 area 1
     (指定参与 OSPF 动态路由项建立过程的网络和接口。Router4~Router6 只参与 OSPF 动
     态路由项建立过程)
Router(config-router)#network 192.1.4.0 0.0.0.255 area 1
Router(config-router)#network 192.1.6.0 0.0.0.255 area 1
Router(config-router)#exit
```

(5) Router5 命令行配置过程。

```
Router>enable
Router# configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.5.1 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 55
Router(config-router)#network 192.1.2.0 0.0.0.255 area 1
Router(config-router)#network 192.1.4.0 0.0.0.255 area 1
Router(config-router)#network 192.1.5.0 0.0.0.255 area 1
Router(config-router)#exit
```

(6) Router6 命令行配置过程。

```
Router>enable
Router# configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.5.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.6.2 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 66
Router(config-router)#network 192.1.3.0 0.0.0.255 area 1
Router(config-router)#network 192.1.6.0 0.0.0.255 area 1
Router(config-router)#network 192.1.5.0 0.0.0.255 area 1
Router(config-router)#exit
```

8.3.2 IP Sec 配置实验

1. 实验内容

(1) 配置 ISAKMP 策略。

(2) 配置 IP Sec 参数。

(3) 验证 IP Sec 安全关联建立过程。

(4) 查看 ESP 报文封装过程。

2. 网络结构

该实验在 8.3.1 节点对点 IP 隧道配置实验基础上进行,采用 IP Sec 协议解决内层 IP 分组经过隧道传输时的保密性和安全性问题。通过 ISAKMP 在隧道两端建立 IP Sec 安全关联,将内层 IP 分组封装成 ESP 报文后,再经过隧道传输。ISAKMP 分两阶段完成隧道两端 IP Sec 安全关联建立过程:第一阶段建立安全传输通道,两端需要约定加密算法、报文摘要算法、鉴别方式和 DH 组号。第二阶段建立 IP Sec 安全关联,两端需要约定安全协议、加密算法和 HMAC 算法。该实验通过配置 ISAKMP 策略约定建立安全传输通道使用的加密算法 3DES、报文摘要算法 MD5、共享密钥鉴别方式和 DH 组号 DH-2。通过配置 IP Sec 变换集约定建立 IP Sec 安全关联时使用的安全协议、加密算法和 HMAC 算法 ESP-3DES 和 ESP-MD5-HMAC。

3. 实验步骤

(1) 在完成 8.3.1 节点对点 IP 隧道配置实验基础上进行该实验,打开完成 8.3.1 节点对点 IP 隧道配置实验的 pkt 文件。

(2) 在隧道两端通过命令"crypto isakmp policy 1"开始 ISKMP 策略配置过程,指定建立安全传输通道使用的加密算法 3DES、报文摘要算法 MD5、共享密钥鉴别方式和 DH 组号 DH-2。隧道每一端可以配置多个 ISAKMP 策略,但两端必须存在匹配的 ISAKMP 策略,否则终止 IP Sec 安全关联建立过程。

(3) 由于双方采用共享密钥鉴别方式,需要为隧道两端配置共享密钥,通过命令"crypto isakmp key 1234 address 0.0.0.0 0.0.0.0"将共享密钥 1234 和另一端 IP 地址绑定在一起,0.0.0.0 0.0.0.0 表示所有 IP 地址,Packet Tracer 只能用单个共享密钥绑定所有采用共享密钥鉴别方式的两端。

(4) 在隧道两端通过命令"crypto ipsec transform－set tunnel esp-3des esp-md5-hmac"指定 IP Sec 安全关联使用的安全协议 ESP、加密算法 3DES 和 HMAC 算法 HMAC-MD5。Tunnel 是该变换集的名字。

(5) 通过配置访问控制列表指定隧道两端需要进行安全传输的 IP 分组范围。

(6) 隧道每一端通过命令"crypto map tunnel 10 ipsec－isakmp"创建加密映射,tunnel 是加密映射名,10 是序号。加密映射中将 IP Sec 安全关联的另一端地址、为 IP Sec 配置的变换集及用于控制需要安全传输的 IP 分组范围的访问控制列表绑定在一起。如果某个端口作为多条隧道的源端口,则需要创建多个名字相同、序号不同的加密映射,每一个加密映射对应不同的隧道。

(7) 在接口配置模式,通过命令"crypto map tunnel"将创建的加密映射作用到该接

口，tunnel 是加密映射名。加密映射一旦作用到某个接口上，按照加密映射的配置，自动建立 IP Sec 安全关联，并通过 IP Sec 安全关联安全传输访问控制列表指定的 IP 分组。

（8）在隧道两端接口使能“各自创建的加密映射”后，隧道两端通过 ISAKMP 自动创建 IP Sec 安全关联，内层 IP 分组可以封装成 ESP 报文经过隧道传输。图 8.21 是图 8.11 中 PC0 至 Server2 的内层 IP 分组，以内部网络本地 IP 地址 192.168.1.1 和 192.168.3.3 为源和目的 IP 地址。图 8.22 是该内层 IP 分组封装成 ESP 报文过程，它首先被封装成 GRE 格式，GRE 格式被封装成 ESP 报文，ESP 报文作为外层 IP 分组的净荷。ESP 采用加密算法 3DES 和 HAMC 算法 HMAC-MD5。

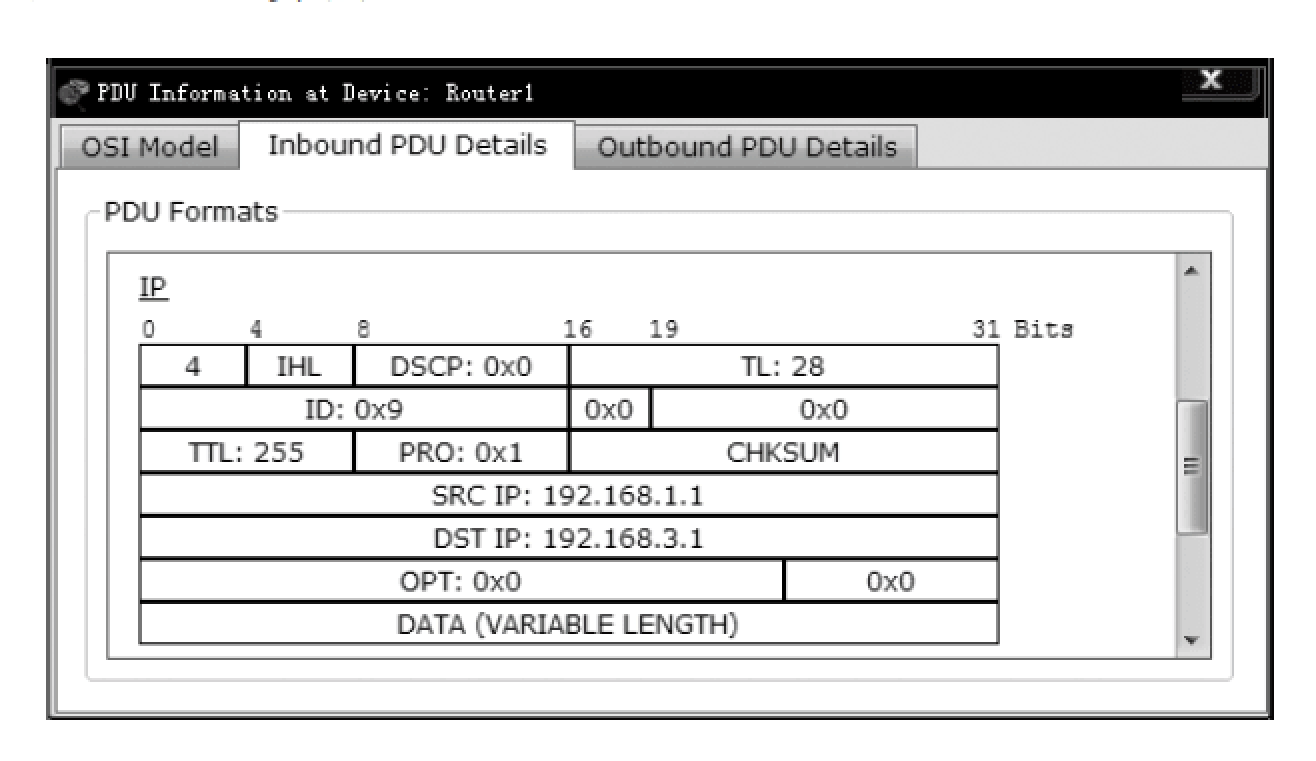


图 8.21　PC0 至 Server2 内层 IP 分组

4. 命令行配置过程

（1）Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#crypto isakmp policy 1        (开始 ISAKMP 策略定义过程，1 是策略编号)
Router(config-isakmp)#authentication pre-share        (采用共享密钥鉴别方式)
Router(config-isakmp)#encryption 3des                 (采用 3DES 加密算法)
Router(config-isakmp)#hash md5                        (采用 MD5 报文摘要算法)
Router(config-isakmp)#group 2                         (采用 DH-2)
Router(config-isakmp)#lifetime 900
                    (IP Sec 安全关联存活时间，一旦经过该时间，将重新建立 IP Sec 安全关联)
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 1234 address 0.0.0.0 0.0.0.0
                              (需要鉴别身份的所有隧道两端有着相同的共享密钥 1234)
Router(config)#crypto ipsec transform-set tunnel esp-3des esp-md5-hmac
               (IP Sec 安全关联两端采用安全协议 ESP、加密算法 3DES、HAMC 算法 HAMC-MD5。
                tunnel 是该变换集名字)
Router(config)#access-list 101 permit gre host 192.1.1.1 host 192.1.2.1
                              (指定隧道 0 加密传输的 IP 分组范围)
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 permit gre host 192.1.1.1 host 192.1.3.1
                              (指定隧道 1 加密传输的 IP 分组范围)
```

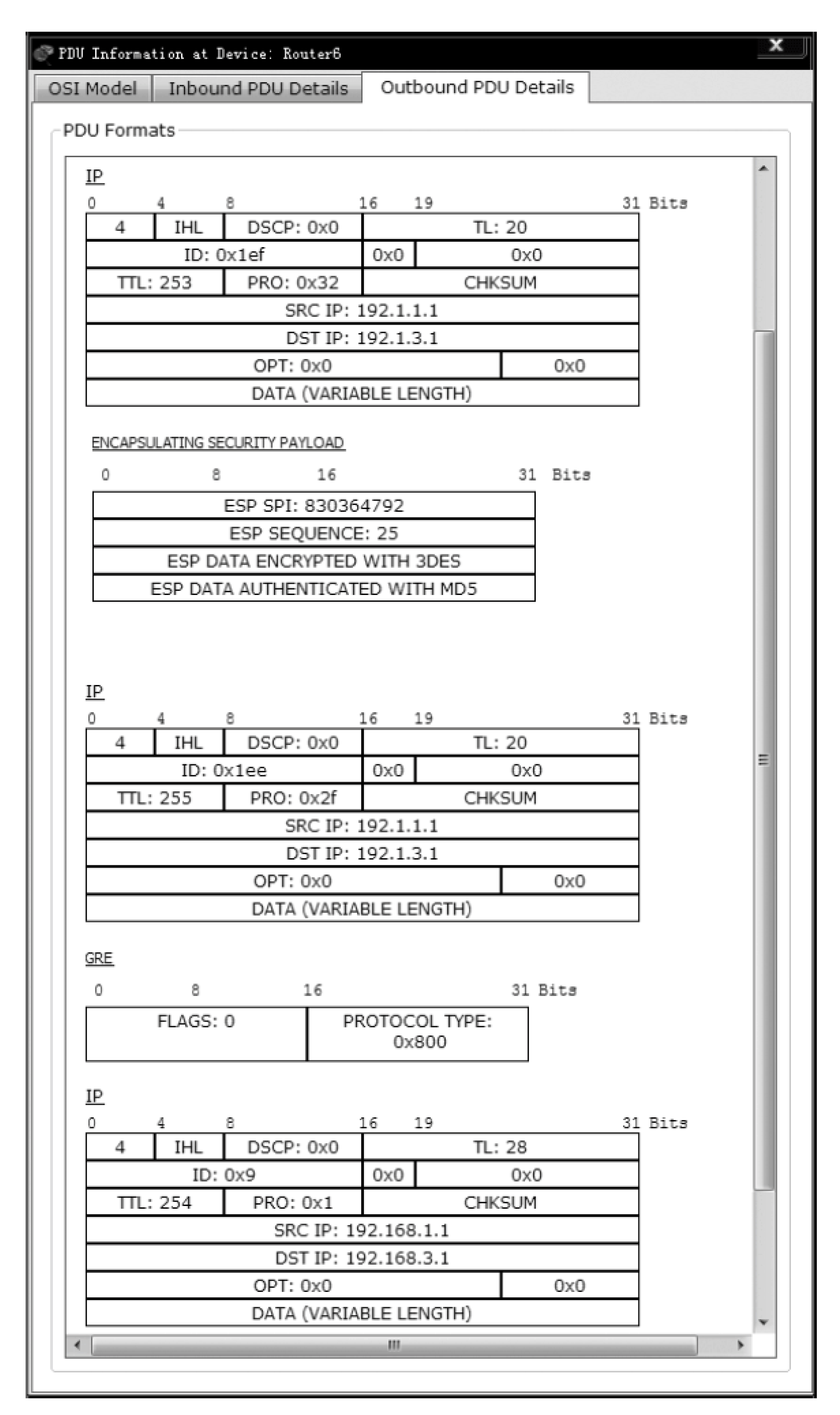


图 8.22 内层 IP 分组封装成 ESP 报文过程

Router(config)#access-list 102 deny ip any any

Router(config)#crypto map tunnel 10 ipsec-isakmp

(创建加密映射，tunnel 是名字，10 是序号。以下是针对隧道 0 的信息)

Router(config-crypto-map)#set peer 192.1.2.1 (指定 IP Sec 安全关联另一端的 IP 地址)

Router(config-crypto-map)#set transform-set tunnel

(通过引用名为 tunnel 的变换集，指定 IP Sec 安全关联相关的参数)

Router(config-crypto-map)#match address 101

(通过引用编号为 101 的访问控制列表，指定需要安全传输的 IP 分组范围)

Router(config-crypto-map)#exit

Router(config)#crypto map tunnel 20 ipsec-isakmp

(如果同一个接口需要作为多条隧道的源端，需要为每一条隧道创建名字相同，序号不同的加密映射。以下是针对隧道 1 的信息)

```
Router(config-crypto-map)#set peer 192.1.3.1
Router(config-crypto-map)#set transform-set tunnel
Router(config-crypto-map)#match address 102
Router(config-crypto-map)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#crypto map tunnel
                              (将名为 tunnel 的加密映射作用到接口 FastEthernet0/1)
Router(config-if)#exit
```

（2）Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#crypto isakmp policy 1     (隧道两端必须配置相互匹配的 ISAKMP 策略)
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 900
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 1234 address 0.0.0.0 0.0.0.0
                    (隧道两端有着相同的共享密钥 1234)
Router(config)#crypto ipsec transform-set tunnel esp-3des esp-md5-hmac
                    (隧道两端配置相同的与 IP Sec 安全关联相关的参数)
Router(config)#access-list 101 permit gre host 192.1.2.1 host 192.1.1.1
                    (通过编号为 101 的访问控制列表,指定经过隧道安全传输的 IP 分组范围)
Router(config)#access-list 101 deny ip any any
Router(config)#crypto map tunnel 10 ipsec-isakmp
                    (创建名为 tunnel 的加密映射,配置以下针对隧道 0 的信息)
Router(config-crypto-map)#set peer 192.1.1.1
Router(config-crypto-map)#set transform-set tunnel
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#crypto map tunnel
Router(config-if)#exit
```

（3）Router3 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 2
```

```
Router(config-isakmp)#lifetime 900
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 1234 address 0.0.0.0 0.0.0.0
Router(config)#crypto ipsec transform-set tunnel esp-3des esp-md5-hmac
Router(config)#access-list 101 permit gre host 192.1.3.1 host 192.1.1.1
Router(config)#access-list 101 deny ip any any
Router(config)#crypto map tunnel 10 ipsec-isakmp
Router(config-crypto-map)#set peer 192.1.1.1
Router(config-crypto-map)#set transform-set tunnel
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#crypto map tunnel
Router(config-if)#exit
```

8.3.3 Cisco Easy VPN 配置实验

1. 实验内容

（1）配置 ISAKMP 策略。

（2）配置 IP Sec 参数。

（3）配置 VPN 服务器。

（4）验证远程接入过程。

（5）查看 ESP 报文封装过程。

2. 网络结构

网络结构如图 8.8 所示。网络由内部网络和 Internet 两部分组成，由路由器 R2 实现互连，路由器 R2 同时又是 VPN 服务器，完成对远程终端的接入控制。配置全球 IP 地址的远程终端在完成远程接入过程前无法访问内部网络资源，完成远程接入后，由 VPN 服务器为远程终端分配内部网络本地 IP 地址，通过完成远程接入过程中建立的远程终端至 VPN 服务器之间的 IP Sec 安全关联，实现以远程终端和内部网络服务器的本地 IP 地址为源和目的 IP 地址的内层 IP 分组经过 Internet 安全传输的功能。

3. 实验步骤

（1）启动 Packet Tracer，在逻辑工作区根据图 8.8 所示的网络结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 8.23 所示。

（2）按照图 8.8 所示各个路由器接口的 IP 地址和子网掩码完成路由器接口 IP 地址和子网掩码配置，在路由器 R1 和 R2 中启动 RIP 进程建立通往内部网络各个子网的传输路径，在路由器 R2 和 R3 中启动 OSPF 进程建立通往 Internet 各个子网的传输路径。路由器 R1～路由器 R3 的路由表如图 8.24～图 8.26 所示。值得指出的是，路由器 R3 路由表中只包含用于指明通往 Internet 各个子网的传输路径的路由项，路由器 R1 路由表中只包含用于指明通往内部网络各个子网的传输路径的路由项，因此配置全球 IP 地址的远程终端 PC2 和 PC3 无法访问内部网络服务器 Web Server。

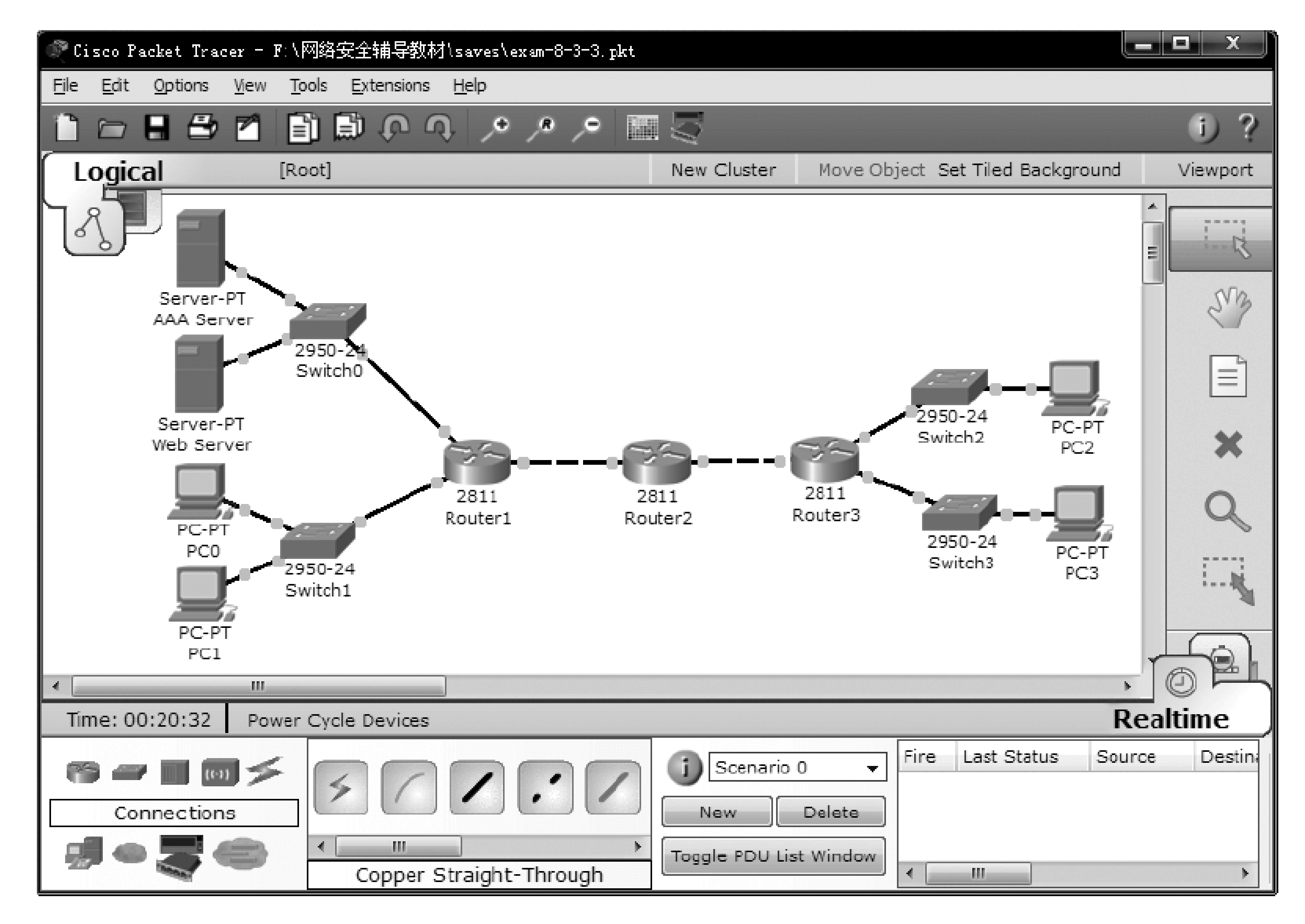
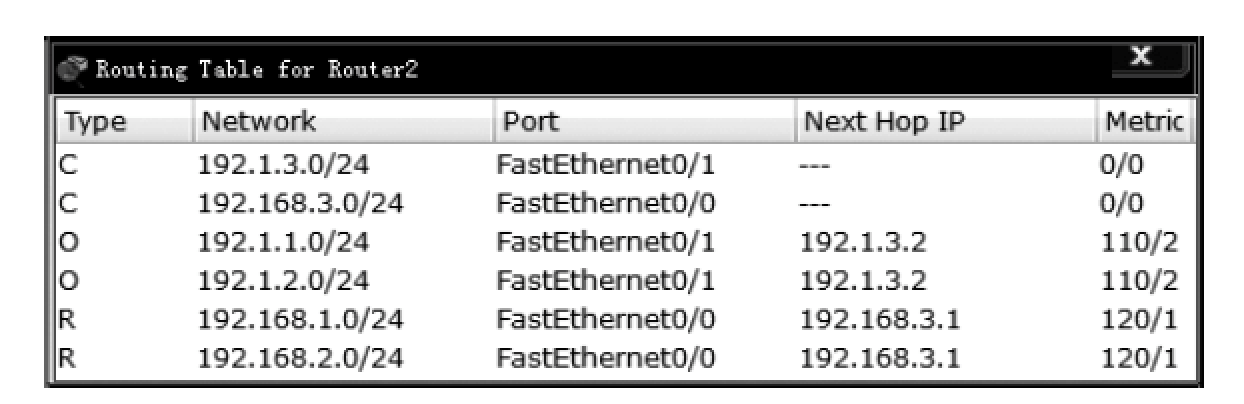


图 8.23　放置和连接设备后的逻辑工作区界面

Routing Table for Router1

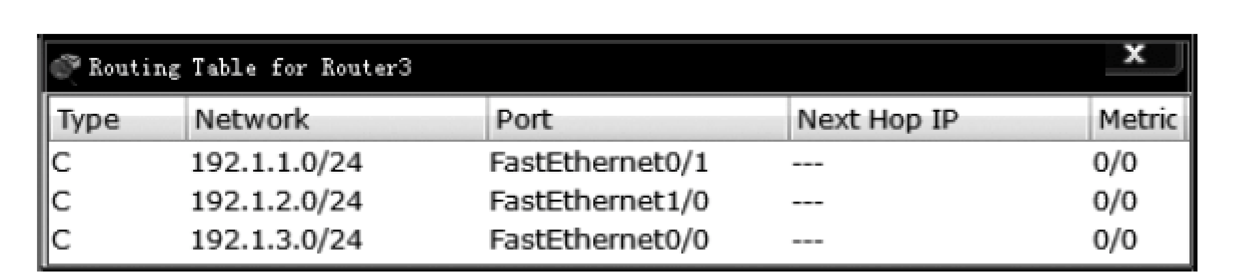
Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0
C	192.168.3.0/24	FastEthernet1/0	---	0/0
S	192.168.4.0/24	---	192.168.3.2	1/0

图 8.24　Router1 路由表


Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	FastEthernet0/1	---	0/0
C	192.168.3.0/24	FastEthernet0/0	---	0/0
O	192.1.1.0/24	FastEthernet0/1	192.1.3.2	110/2
O	192.1.2.0/24	FastEthernet0/1	192.1.3.2	110/2
R	192.168.1.0/24	FastEthernet0/0	192.168.3.1	120/1
R	192.168.2.0/24	FastEthernet0/0	192.168.3.1	120/1

图 8.25　Router2 路由表


Routing Table for Router3

Type	Network	Port	Next Hop IP	Metric
C	192.1.1.0/24	FastEthernet0/1	---	0/0
C	192.1.2.0/24	FastEthernet1/0	---	0/0
C	192.1.3.0/24	FastEthernet0/0	---	0/0

图 8.26　Router3 路由表

(3) 完成 VPN 服务器(路由器 Router2)的配置,配置内容分为三部分:一是和建立 IP Sec 安全关联相关的配置,包括 ISAKMP 策略、IP Sec 变换集和加密映射,只是由于无法确定 IP Sec 安全关联的另一端,必须建立动态加密映射。二是远程终端组配置,为属于该远程终端组的远程终端配置共享密钥、内部网络本地 IP 地址池、子网掩码及其他网络配置信息。三是配置远程接入用户身份鉴别信息,配置 RADIUS 服务器信息

(RADIUS 服务器 IP 地址和传输密钥),并在 AAA 服务器配置授权用户身份标识信息,AAA 服务器配置界面如图 8.27 所示。

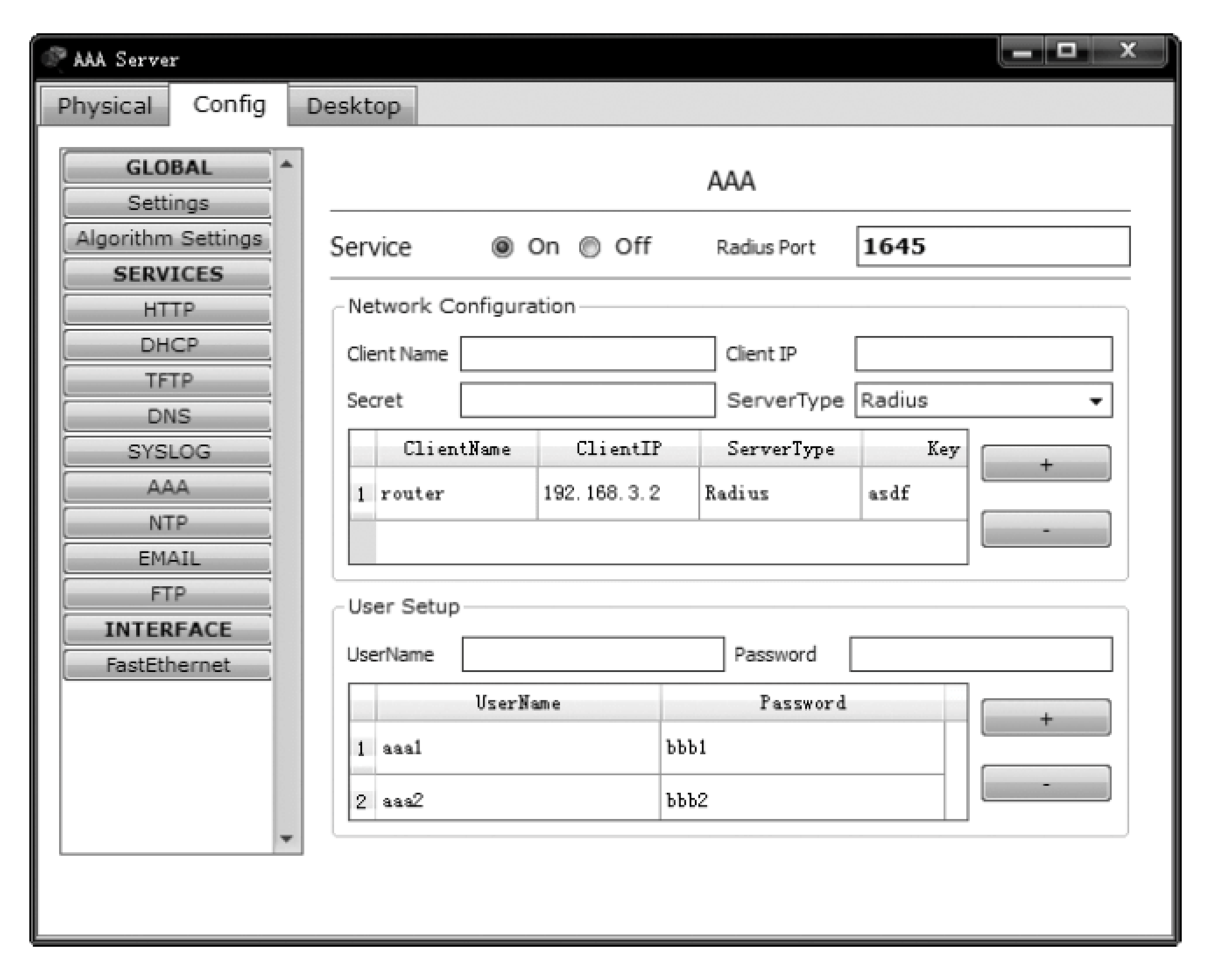


图 8.27　AAA 服务器配置界面

(4) 完成 VPN 服务器和 AAA 服务器配置后,通过启动 VPN 客户端程序开始远程接入过程,图 8.28 所示为 PC2 的 VPN 客户端配置界面,组名(Group Name)是在 VPN 服务器配置终端组时指定的终端组名字,组密钥(Group Key)为该终端组配置的共享密钥,VPN 服务器 IP 地址(Server IP)是路由器 R2 作用加密映射的接口的全球 IP 地址。用户名(Username)和口令(Password)必须是 AAA 服务器中配置的某个授权用户的用户标识信



图 8.28　PC2 VPN 客户端配置界面

息。一旦终端远程接入成功，终端被分配内部网络本地 IP 地址。图 8.29 所示是 PC2 成功完成远程接入后分配的内部网络本地 IP 地址，它属于 VPN 服务器定义的本地 IP 地址池。VPN 为远程终端分配内部网络本地 IP 地址的同时，建立以该内部网络本地 IP 地址为目的地址的路由项，路由项将该内部网络本地 IP 地址和 VPN 与远程终端之间的安全隧道绑定在一起，因此该路由项的下一跳是安全隧道另一端的全球 IP 地址，即该远程终端配置的全球 IP 地址。路由器 R2 在完成 PC2 和 PC3 远程接入后的路由表如图 8.30 所示。



图 8.29　PC2 远程接入后分配的内部网络本地 IP 地址

Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	FastEthernet0/1	---	0/0
C	192.168.3.0/24	FastEthernet0/0	---	0/0
O	192.1.1.0/24	FastEthernet0/1	192.1.3.2	110/2
O	192.1.2.0/24	FastEthernet0/1	192.1.3.2	110/2
R	192.168.1.0/24	FastEthernet0/0	192.168.3.1	120/1
R	192.168.2.0/24	FastEthernet0/0	192.168.3.1	120/1
S	192.168.4.1/32	FastEthernet0/1	192.1.1.1	1/0
S	192.168.4.2/32	FastEthernet0/1	192.1.2.1	1/0

图 8.30　Router2 中增加的以远程接入终端为目的终端的路由项

(5) PC2 成功完成远程接入后，可以访问内部网络服务器，图 8.31 是 PC2 成功访问 Web Server 的界面。

(6) PC2 至 Web Server 的 IP 分组以 PC2 内部网络本地 IP 地址 192.168.4.1 为源 IP 地址，以 Web Server 内部网络本地 IP 地址 192.168.1.2 为目的 IP 地址，这样的 IP 分组无法完成 PC2 至路由器 R2 这一段 Internet 传输路径的传输过程，因此必须封装成以 PC2 全球 IP 地址 192.1.1.1 为源 IP 地址，路由器 R2 全球 IP 地址 192.1.3.1 为目的 IP 地址的外层 IP 分组格式。为了实现内层 IP 分组经过 Internet 的可靠传输，内层 IP 分组首先被封装成 ESP 报文，整个封装过程涉及的内层 IP 分组格式、ESP 报文格式、UDP 报文格式及外层 IP 分组格式如图 8.32 所示。

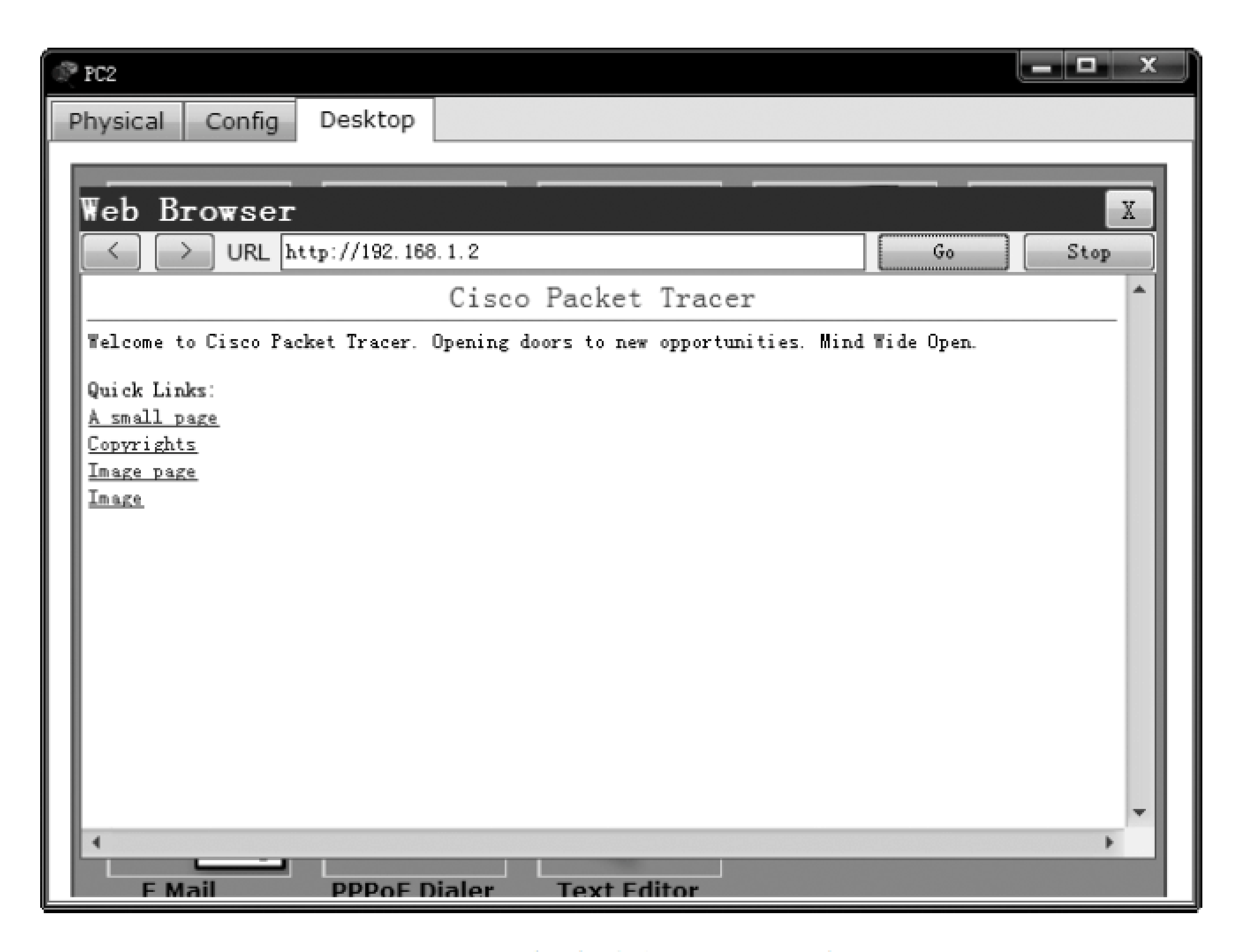


图 8.31 PC2 成功访问 Web 服务器界面

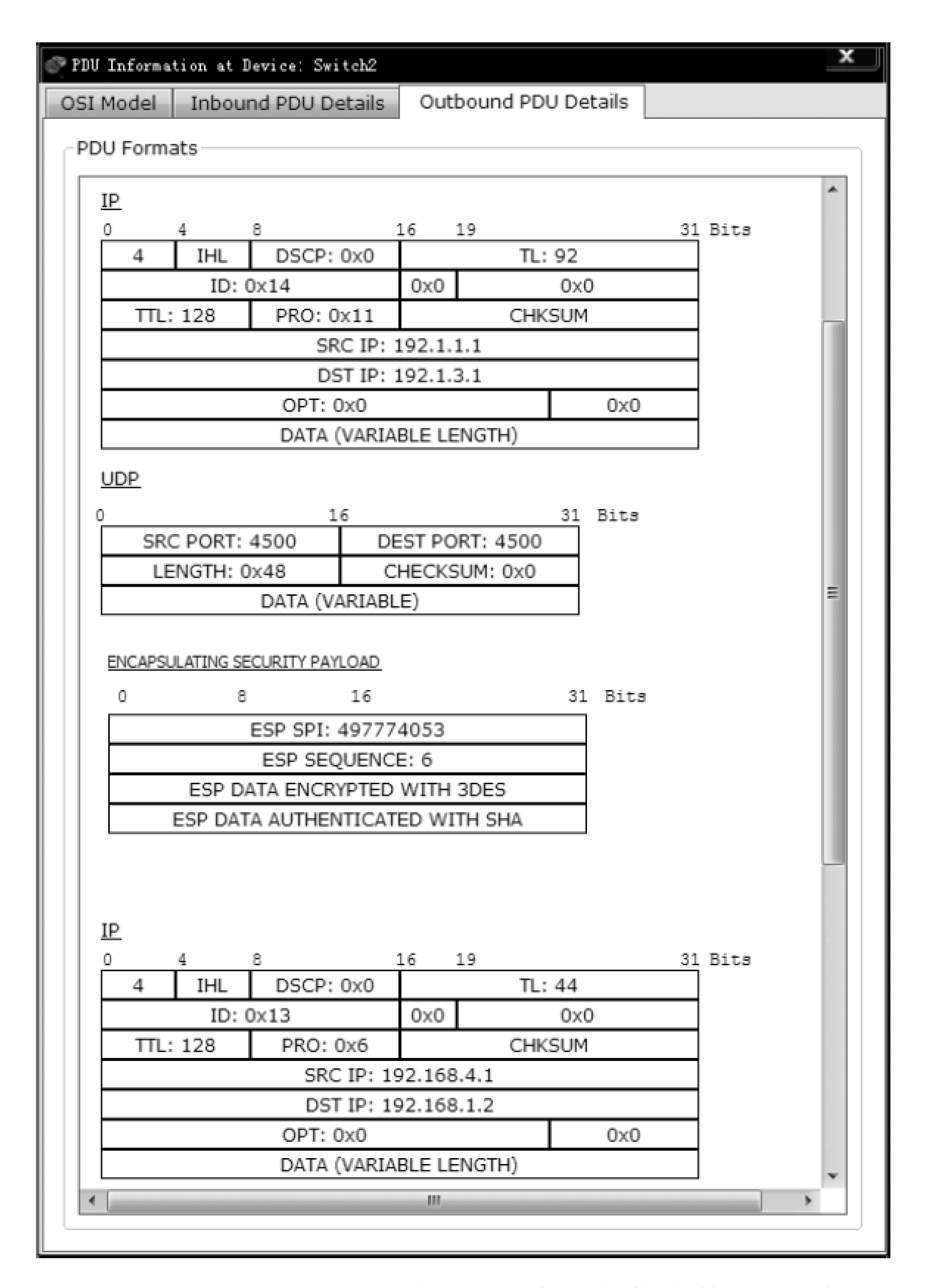


图 8.32 PC2 至 Web 服务器内层 IP 分组封装成外层 IP 分组过程

(7) VPN 服务器从到达的外层 IP 分组中分离出内层 IP 分组，然后经过内部网络将内层 IP 分组传输给 Web Server。经过内部网络传输的内层 IP 分组格式如图 8.33 所示。

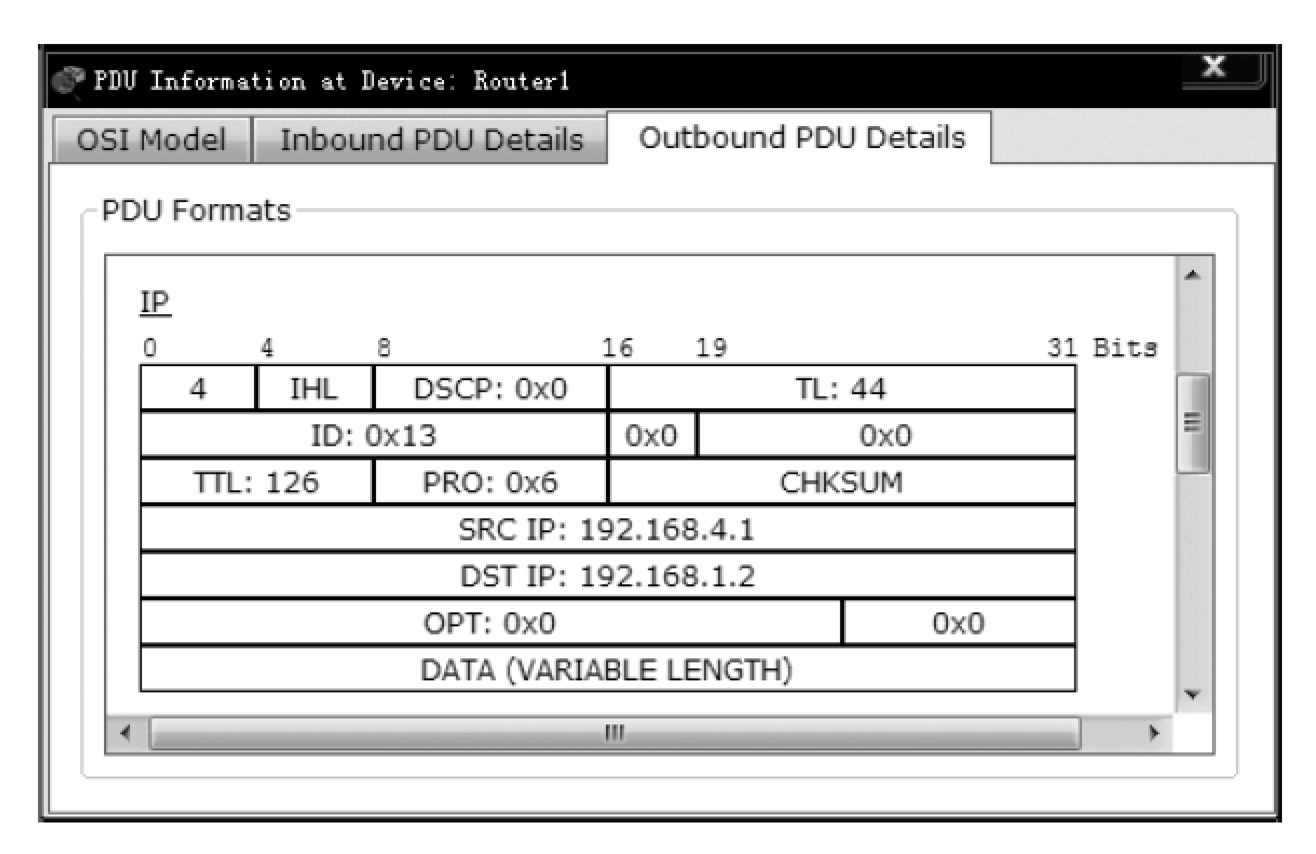


图 8.33　经过内部网络传输的 PC2 至 Web 服务器内层 IP 分组

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#exit
```

(2) Router2 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
```

```
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 22
Router(config-router)#network 192.1.3.0 0.0.0.255 area 1
Router(config-router)#exit
Router(config)#crypto isakmp policy 1            (开始 ISAKMP 策略定义过程,1是策略编号)
Router(config-isakmp)#authentication pre-share   (采用共享密钥鉴别方式)
Router(config-isakmp)#encryption aes 256         (采用256位AES加密算法)
Router(config-isakmp)#hash sha                   (采用SHA报文摘要算法)
Router(config-isakmp)#group 2         (采用DH-2。这是Cisco Easy VPN约定的DH组号)
Router(config-isakmp)#lifetime 900
        (IP Sec安全关联存活时间,一旦经过该时间,将重新建立IP Sec安全关联。重新建立IP
        Sec安全关联过程由VPN服务器发起)
Router(config-isakmp)#exit
Router(config)#crypto isakmp client configuration group asdf
        (配置远程客户组,asdf是组名。如果某个远程终端属于该客户组,需要在VPN客户端配
        置界面输入该组名)
Router(config-isakmp-group)#key asdf             (配置共享密钥asdf)
Router(config-isakmp-group)#pool vpnpool
    (配置用于为属于该客户组的远程终端分配的内部网络本地IP地址池,vpnpool是地址池名)
Router(config-isakmp-group)#netmask 255.255.255.0
                            (配置用于为属于该客户组的远程终端分配的子网掩码)
Router(config-isakmp-group)#exit
Router(config)#crypto ipsec transform-set vpnt esp-3des esp-sha-hmac
        (IP Sec安全关联两端采用安全协议ESP、加密算法3DES、HAMC算法HAMC-SHA。vpnt是该
        变换集名字)
Router(config)#crypto dynamic-map vpn 10
        (创建动态加密映射,vpn是名字,10是序号。动态加密映射可以不需要配置IP Sec安全
        关联另一端的IP地址)
Router(config-crypto-map)#set transform-set vpnt
                            (通过引用名为vpnt的变换集,指定IP Sec安全关联相关的参数)
Router(config-crypto-map)#reverse-route
      (一旦建立与远程终端之间的安全关联,需要在VPN服务器的路由表中创建将该远程终端
      内部网络本地IP地址和VPN服务器与该远程终端之间安全隧道绑定在一起的路由项)
Router(config-crypto-map)#exit
Router(config)#aaa new-model
```

```
Router(config)#aaa authentication login vpna group radius
        (指定远程接入用户的身份鉴别机制,vpna 是机制名,该机制要求通过 RADIUS 服务器完
        成远程接入用户的身份鉴别)
Router(config)#aaa authorizatio network vpnb local
(指定访问内部网络的授权机制,vpnb 是机制名)
Router(config)#radius-server host 192.168.1.1      (配置 RADIUS 服务器 IP 地址)
Router(config)#radius-server key asdf
                    (配置 VPN 服务器与 RADIUS 服务器之间的共享密钥)
Router(config)#hostname router                     (配置 VPN 服务器主机名)
router(config)#crypto map vpn client authentication list vpna
                    (将名为 vpna 的鉴别机制与名为 vpn 的加密映射绑定在一起)
router(config)#crypto map vpn isakmp authorization list vpnb
                    (将名为 vpnb 的授权机制与名为 vpn 的加密映射绑定在一起)
router(config)#crypto map vpn client configuration address respond
   (可以用请求者的 IP 地址作为 IP Sec 安全关联另一端的 IP 地址。这是动态加密映射必须的)
router(config)#crypto map vpn 10 ipsec-isakmp dynamic vpn
                    (将名为 vpn 的动态加密映射作为启动 ISAKMP 和 IP Sec 的加密映射)
router(config)#ip local pool vpnpool 192.168.4.1 192.168.4.100
                    (配置内部网络本地 IP 地址池,vpnpool 是地址池名)
router(config)#interface FastEthernet0/1
router(config-if)#crypto map vpn    (将名为 vpn 的加密映射作用到接口 FastEthernet0/1)
router(config-if)#exit
```

(3) Router3 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 33
Router(config-router)#network 192.1.1.0 0.0.0.255 area 1
Router(config-router)#network 192.1.2.0 0.0.0.255 area 1
Router(config-router)#network 192.1.3.0 0.0.0.255 area 1
Router(config-router)#exit
```

第9章 防火墙

CHAPTER

9.1 知识要点

9.1.1 无状态分组过滤器

1. 过滤规则

无状态分组过滤器通过规则从IP分组流中鉴别出一组IP分组，然后对其实施规定的操作。规则由一组属性值组成，如果某个IP分组携带的信息和构成规则的一组属性值匹配，意味着该IP分组和该规则匹配，对该IP分组实施相关操作，相关操作有正常转发和丢弃。

构成规则的属性值通常由下述字段组成：

- 源IP地址：用于匹配IP分组IP首部中的源IP地址字段值。
- 目的IP地址：用于匹配IP分组IP首部中的目的IP地址字段值。
- 源和目的端口号：用于匹配作为IP分组净荷的传输层报文首部中源和目的端口号字段值。
- 协议类型：用于匹配IP分组首部中的协议字段值。

一个过滤器可以由多个规则构成，IP分组只有和当前规则不匹配时，才继续和后续规则进行匹配操作。如果和过滤器中的所有规则都不匹配，对IP分组进行默认操作。IP分组一旦和某个规则匹配，则对其实施相关操作，不再和其他规则进行匹配操作，因此IP分组和规则的匹配操作顺序直接影响该IP分组所匹配的规则，也因此确定了对该IP分组实施的操作。

无状态分组过滤器可以作用于接口的输入或输出方向，输入或输出方向针对无状态分组过滤器而言，从外部进入无状态分组过滤器称为输入，离开无状态分组过滤器称为输出。如果作用于输入方向，每一个输入IP分组都和过滤器中的规则进行匹配操作，如果和某个规则匹配，则对其实施相关操作，如果实施的操作是丢弃，不再对该IP分组进行后续的转发处理。如果过滤器作用于输出方向，则只有当该IP分组确定从该接口输出时，才将该IP分组和过滤器中的规则进行匹配操作。

2. 过滤规则举例

网络结构如图 9.1 所示。分别写出作用于路由器 R1 接口 1 输入方向，路由器 R2 接口 2 输入方向，实现只允许终端 A 访问 Web 服务器，终端 B 访问 FTP 服务器，禁止其他一切通信的访问控制的过滤规则。

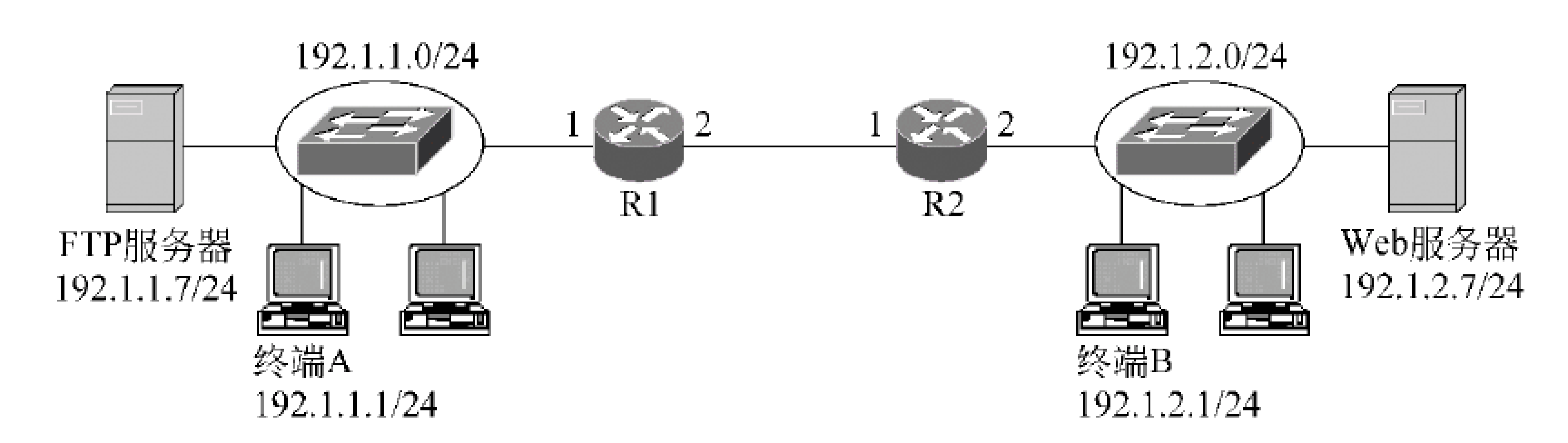


图 9.1 网络结构

路由器 R1 接口 1 输入方向过滤规则如下：

① 协议=TCP，源 IP 地址=192.1.1.1/32，源端口号=＊，目的 IP 地址=192.1.2.7/32，目的端口号=80；正常转发。

② 协议=TCP，源 IP 地址=192.1.1.7/32，源端口号=20，目的 IP 地址=192.1.2.1/32，目的端口号=＊；正常转发。

③ 协议=TCP，源 IP 地址=192.1.1.7/32，源端口号=21，目的 IP 地址=192.1.2.1/32，目的端口号=＊；正常转发。

④ 协议=IP，源 IP 地址=＊，目的 IP 地址=＊；丢弃。

路由器 R2 接口 2 输入方向过滤规则如下：

① 协议=TCP，源 IP 地址=192.1.2.1/32，源端口号=＊，目的 IP 地址=192.1.1.7/32，目的端口号=20；正常转发。

② 协议=TCP，源 IP 地址=192.1.2.1/32，源端口号=＊，目的 IP 地址=192.1.1.7/32，目的端口号=21；正常转发。

③ 协议=TCP，源 IP 地址=192.1.2.7/32，源端口号=80，目的 IP 地址=192.1.1.1/32，目的端口号=＊；正常转发。

④ 协议=IP，源 IP 地址=＊，目的 IP 地址=＊；丢弃。

路由器 R1 接口 1 输入方向过滤规则①表明只允许终端 A 以 HTTP 访问 Web 服务器的 TCP 报文继续正常转发。过滤规则②表明只允许属于 FTP 服务器和终端 B 之间控制连接的 TCP 报文继续正常转发。过滤规则③表明只允许属于 FTP 服务器和终端 B 之间数据连接的 TCP 报文继续正常转发。过滤规则④表明丢弃所有不符合上述过滤规则的 IP 分组。路由器 R2 接口 2 输入方向过滤规则的作用与此相似。

3. Cisco 访问控制列表实现

路由器 R1 接口 1 输入方向配置的 Cisco 访问控制列表如下：

```
access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq 80
access-list 101 permit tcp host 192.1.1.7 eq 20 host 192.1.2.1
access-list 101 permit tcp host 192.1.1.7 eq 21 host 192.1.2.1
```

```
access-list 101 deny ip any any
```

上述访问控制列表中 101 是编号，属于同一访问控制列表的过滤规则必须具有相同的编号。permit 是实施的操作，允许正常转发。tcp 是协议类型，表示是 TCP 报文。host 192.1.1.1 表示源 IP 地址为 192.1.1.1/32。如果源 IP 地址为网络地址 192.1.1.0/24，需用 192.1.1.0 0.0.0.255 表示，其中 192.1.1.0 是网络地址，0.0.0.255 是子网掩码 255.255.255.0 的反码。host 192.1.2.7 表示目的 IP 地址为 192.1.2.7/32。紧随源 IP 地址的是源端口号，紧随目的 IP 地址的是目的端口号，所以上述访问控制列表中，eq 80 表示目的端口号等于 80，eq 20 表示源端口号等于 20。deny 是拒绝操作，丢弃该 IP 分组。any 表示任意 IP 地址，也可用 0.0.0.0 255.255.255.255 表示，这里 0.0.0.0 表示任意网络，255.255.255.255 表示网络前缀位数是 0。以此得出，host 192.1.1.1 可以表示为 192.1.1.1 0.0.0.0，0.0.0.0 表示网络前缀位数是 32。

Cisco 访问控制列表的默认过滤规则是过滤规则④，因此配置 Cisco 访问控制列表时，无需配置过滤规则④。

路由器 R2 接口 2 输入方向配置的 Cisco 访问控制列表如下：

```
access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 eq 20
access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 eq 21
access-list 102 permit tcp host 192.1.2.7 eq 80 host 192.1.1.1
access-list 102 deny ip any any
```

9.1.2　有状态分组过滤器

1. 有状态分组过滤器实现原理

如果要求实现只允许终端 A 发起访问 Web 服务器，不允许网络存在其他通信过程的访问控制，路由器 R1 接口 1 输入方向和路由器 R2 接口 2 输入方向设置如下过滤规则。

路由器 R1 接口 1 输入方向过滤规则如下：

① 协议＝TCP，源 IP 地址＝192.1.1.1/32，源端口号＝*，目的 IP 地址＝192.1.2.7/32，目的端口号＝80；正常转发。

② 协议＝IP，源 IP 地址＝*，目的 IP 地址＝*；丢弃。

路由器 R2 端口 2 输入方向过滤规则如下：

① 协议＝TCP，源 IP 地址＝192.1.2.7/32，源端口号＝80，目的 IP 地址＝192.1.1.1/32，目的端口号＝*；正常转发。

② 协议＝IP，源 IP 地址＝*，目的 IP 地址＝*；丢弃。

需要强调的是，真正实现只允许终端 A 发起访问 Web 服务器，不允许网络存在其他通信过程的访问控制需要做到：①只允许由终端 A 发起建立与 Web 服务器之间的 TCP 连接。②只允许属于由终端 A 发起建立的与 Web 服务器之间的 TCP 连接的 TCP 报文沿着 Web 服务器至终端 A 方向传输。③必须由终端 A 发出访问 Web 服务器资源的请求消息，然后由 Web 服务器返回对应的响应消息。

但上述过滤规则中直接允许 Web 服务器发送的、源端口号为 80 的 TCP 报文沿着 Web 服务器至终端 A 方向传输，一是没有规定这种传输过程必须在由终端 A 发起建立与 Web 服务器之间的 TCP 连接后进行；二是由于需要用两端插口标识 TCP 连接，因此上述过滤规则并没有明确指出只有属于由终端 A 发起建立与 Web 服务器之间的 TCP 连接的 TCP 报文才能沿着 Web 服务器至终端 A 方向传输；三是没有检测 Web 服务器传输给终端 A 的 TCP 报文是否是终端 A 发送的请求消息对应的响应消息。

真正实现只允许终端 A 发起访问 Web 服务器，不允许网络存在其他通信过程的访问控制的思路应该这样：①终端 A 至 Web 服务器传输方向上的过滤规则允许传输与完成由终端 A 发起访问 Web 服务器的操作有关的 TCP 报文。②初始状态下，Web 服务器至终端 A 传输方向上的过滤规则拒绝一切 IP 分组传输。③只有当终端 A 至 Web 服务器传输方向上传输了与终端 A 发起访问 Web 服务器的操作有关的 TCP 报文后，Web 服务器至终端 A 传输方向才允许传输作为对应响应消息的 TCP 报文。

2. Cisco 有状态分组过滤器实现机制

针对图 9.1 所示的网络结构，Cisco 通过访问控制列表允许与终端 A 访问 Web 服务器有关的 TCP 报文沿着终端 A 至 Web 服务器方向传输，但通过访问控制列表阻止一切 TCP 报文沿着 Web 服务器至终端 A 方向传输。但在终端 A 至 Web 服务器方向启动检测(Inspect)机制，一旦检测到与终端 A 访问 Web 服务器有关的 TCP 报文，在反方向(Web 服务器至终端 A 方向)动态增加允许该 TCP 报文对应的响应报文传输的过滤规则。这样，通过访问控制列表允许与终端 A 访问 Web 服务器有关的 TCP 报文沿着终端 A 至 Web 服务器方向传输，通过检测机制允许作为该 TCP 报文的响应报文沿着 Web 服务器至终端 A 方向传输。允许沿着 Web 服务器至终端 A 方向传输的 TCP 报文必须是访问控制列表允许沿着终端 A 至 Web 服务器方向传输的 TCP 报文的响应报文。

路由器 R1 接口 1 输入方向和路由器 R2 接口 2 输出方向(终端 A 至 Web 服务器传输方向)设置如下访问控制列表：

```
access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www
```

该访问控制列表允许源 IP 地址＝192.1.1.1/32、目的 IP 地址＝192.1.2.7/32、源端口号任意、目的端口号＝HTTP 对应的著名端口号(80)的 TCP 报文正常转发。

路由器 R1 端口 1 输出方向和路由器 R2 接口 2 输入方向(Web 服务器至终端 A 传输方向)设置如下访问控制列表：

```
access-list 102 deny ip any any
```

该访问控制列表禁止一切 IP 分组继续传输。

但需要创建如下检测机制：

```
ip inspect name a101 http
```

a101 是检测机制名，http 是需要检测的应用层协议，该检测机制表示如果在指定方向检测到属于 http 且该方向访问控制列表允许正常转发的 TCP 报文，在相反方向动态增加允许该 TCP 报文对应的响应报文正常转发的过滤规则。

该检测机制必须作用在路由器 R1 接口 1 输入方向和路由器 R2 接口 2 输出方向。

3. Cisco 有状态分组过滤器配置实例

针对图 9.2 所示的网络结构，要求配置实现满足下列访问控制策略的 Cisco 有状态分组过滤器。

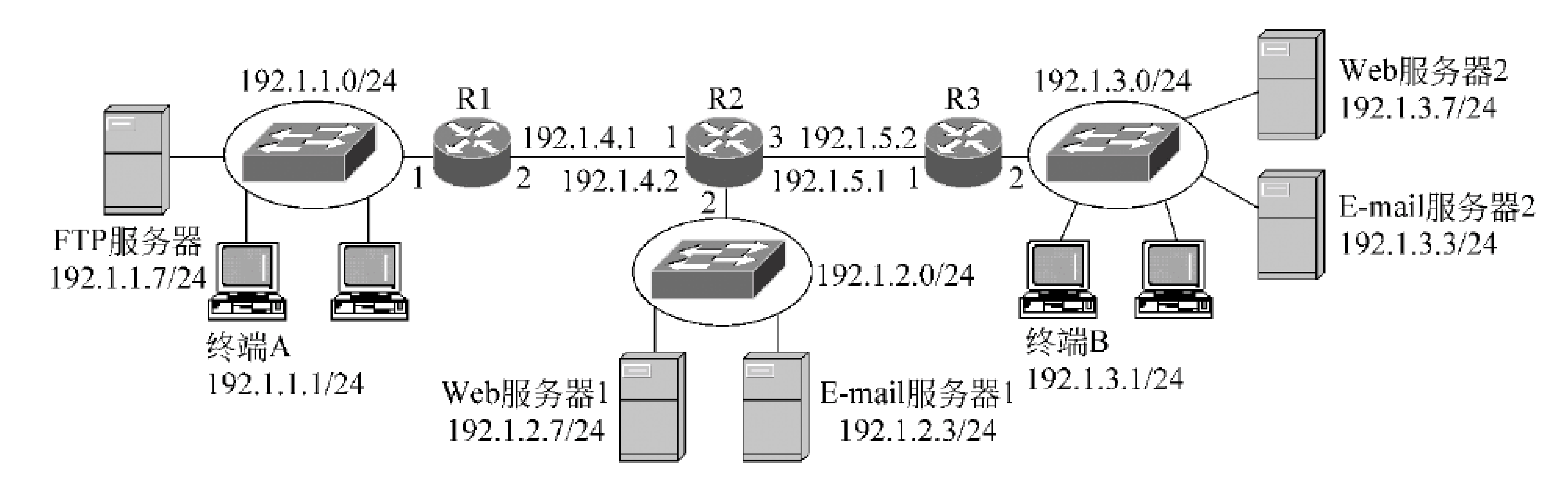


图 9.2　配置 Cisco 有状态分组过滤器的网络结构

① 允许网络 192.1.1.0/24 中的终端访问 Web 服务器 1；
② 允许网络 192.1.1.0/24 中的终端访问 E-mail 服务器 1(SMTP+POP3)；
③ 允许网络 192.1.1.0/24 中的终端访问 Web 服务器 2；
④ 允许 E-mail 服务器 1 访问 E-mail 服务器 2(SMTP)；
⑤ 允许网络 192.1.3.0/24 中的终端访问 Web 服务器 1；
⑥ 允许 E-mail 服务器 2 访问 E-mail 服务器 1(SMTP)。

(1) 配置原则。

Cisco 实现有状态分组过滤器的技术是基于上下文的访问控制(Context-Based Access Control，CBAC)，其思路就是对于任何访问过程，访问控制列表允许与访问过程相关的 TCP 报文沿着发起访问的传输方向继续传输，但在同方向配置检测该访问过程相关应用层协议的检测机制。相反方向通过配置访问控制列表拒绝任何 TCP 报文传输。

对于访问控制策略①和②，路由器 R2 接口 1 输入方向和接口 2 输出方向配置以下访问控制列表和检测机制。

访问控制列表：

```
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq pop3
```

检测机制：

```
ip inspect name a111 http
ip inspect name a111 smtp
ip inspect name a111 pop3
```

对于访问控制策略③，路由器 R2 接口 1 输入方向和接口 3 输出方向配置以下访问控制列表和检测机制。

访问控制列表：

```
access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7 eq www
```

检测机制：

```
ip inspect name a121 http
```

对于访问控制策略④和⑤，路由器 R2 接口 3 输入方向和接口 2 输出方向配置以下访问控制列表和检测机制。

访问控制列表：

```
access-list 131 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7 eq www
access-list 131 permit tcp host 192.1.3.3 host 192.1.2.3 eq smtp
```

检测机制：

```
ip inspect name a131 http
ip inspect name a131 smtp
```

对于访问控制策略⑥，路由器 R2 接口 2 输入方向和接口 3 输出方向配置以下访问控制列表和检测机制。

访问控制列表：

```
access-list 141 permit tcp host 192.1.2.3 host 192.1.3.3 eq smtp
```

检测机制：

```
ip inspect name a141 smtp
```

（2）接口实际配置。

综合上述情况，路由器 R2 各个接口输入输出方向的配置如下。

接口 1 输入方向配置如下。

访问控制列表：

```
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq pop3
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7 eq www
```

检测机制：

```
ip inspect name a111 http
ip inspect name a111 smtp
ip inspect name a111 pop3
```

接口 1 输出方向配置如下。

```
access-list 112 deny ip any any
```

接口 2 输入方向配置如下。

访问控制列表：

```
access-list 122 permit tcp host 192.1.2.3 host 192.1.3.3 eq smtp
```

检测机制：

```
ip inspect name a122 smtp
```

接口 2 输出方向配置如下。
访问控制列表：

```
access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www
access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq pop3
access-list 121 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7 eq www
access-list 121 permit tcp host 192.1.3.3 host 192.1.2.3 eq smtp
```

检测机制：

```
ip inspect name a121 http
ip inspect name a121 smtp
ip inspect name a121 pop3
```

接口 3 输入方向配置如下。
访问控制列表：

```
access-list 132 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7 eq www
access-list 132 permit tcp host 192.1.3.3 host 192.1.2.3 eq smtp
```

检测机制：

```
ip inspect name a132 http
ip inspect name a132 smtp
```

接口 3 输出方向配置如下。
访问控制列表：

```
access-list 131 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7 eq www
access-list 131 permit tcp host 192.1.2.3 host 192.1.3.3 eq smtp
```

检测机制：

```
ip inspect name a131 http
ip inspect name a131 smtp
```

需要强调的是，由于 Packet Tracer 5.3 检测机制不支持应用层协议 SMTP 和 POP3，这两种应用层协议的检测机制只能通过检测 TCP 传输层协议代替。虽然可以用传输层协议 TCP 代替所有基于 TCP 的应用层协议，但检测的内容不同，应用层协议检测机制检测与应用层协议相关的信息，如 HTTP 请求报文中的 URI，响应报文中的插件等，而 TCP 检测机制只检测传输层协议相关信息，如端口号、序号等。

9.1.3 Cisco 区域策略防火墙

1. 实现原理

对于图 9.2 所示的网络结构，区域防火墙的功能：一是将路由器接口分为若干区域，二是对区域间传输的信息流实施控制。

(1) 创建区域。

可以将图 9.2 中的路由器 R2 三个接口连接的三部分网络定义为三个不同的区域：信任区(trust)、非军事区(dmz)和非信任区(notrust)，其中接口 1 连接信任区，接口 2 连接非军事区，接口 3 连接非信任区。这样，9.1.2 节中针对图 9.2 指定的访问控制策略可以变换如下：

① 信任区至非军事区，地址属于 192.1.1.0/24 中的终端通过 HTTP 访问地址为 192.1.2.7/32 的 Web 服务器 1。

② 信任区至非军事区，地址属于 192.1.1.0/24 中的终端通过 SMTP 和 POP3 访问地址为 192.1.2.3/32 的 E-mail 服务器 1。

③ 信任区至非信任区，地址属于 192.1.1.0/24 中的终端通过 HTTP 访问地址为 192.1.3.7/32 的 Web 服务器 2。

④ 非军事区至非信任区，地址为 192.1.2.3/32 的 E-mail 服务器 1 通过 SMTP 访问地址为 192.1.3.3/32 的 E-mail 服务器 2。

⑤ 非信任区至非军事区，地址属于 192.1.3.0/24 中的终端通过 HTTP 访问地址为 192.1.2.7/32 的 Web 服务器 1。

⑥ 非信任区至非军事区，地址为 192.1.3.3/32 的 E-mail 服务器 2 通过 SMTP 访问地址为 192.1.2.3/32 的 E-mail 服务器 1。

(2) 将路由器接口分配给区域。

需要将路由器接口 1 分配给信任区，接口 2 分配给非军事区，接口 3 分配给非信任区。

(3) 分类信息流。

可以通过访问控制列表和应用层协议分类区域间传输的信息流，可以通过下列访问控制列表和应用层协议分类信任区至非军事区的信息流。

```
access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7.and. http
access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3.and. smtp
access-list 101 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3.and. pop3
```

可以通过下列访问控制列表和应用层协议分类信任区至非信任区的信息流。

```
access-list 102 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7.and. http
```

可以通过下列访问控制列表和应用层协议分类非军事区至非信任区的信息流。

```
access-list 103 permit tcp host 192.1.2.3 host 192.1.3.3.and. smtp
```

可以通过下列访问控制列表和应用层协议分类非信任区至非军事区的信息流。

```
access-list 104 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7.and. http
access-list 104 permit tcp host 192.1.3.3 host 192.1.2.3 .and. smtp
```

(4) 定义策略。

访问控制策略就是为每一类信息流定义相应的操作。Cisco 可以为每一类信息流定义的操作有丢弃(Drop)、通过(Pass)和检测(Inspect)。丢弃就是丢弃某类信息流，不允许其继续传输。通过是允许该类信息流继续传输，但只是允许其单向传输，如果某个访问过程涉及双向数据交换，需要在两个传输方向定义操作时通过的策略。检测是既允许信息流单向传输，又允许对应的响应报文反向传输的一种允许某个访问过程涉及的双向数据交换过程进行的操作。对于上述定义的信息流，操作是检测。

(5) 将策略作用到区域间信息流。

定义一对区域，根据传输方向分为源区域和目的区域，通过分类指定区域间传输的信息流类型，对每一类信息流施加操作。

2. 配置过程

(1) 创建区域。

通过以下命令创建三个名字分别为 trust、notrust 和 dmz 的区域。

```
zone security trust
zone security notrust
zone security dmz
```

(2) 将路由器接口分配给区域。

分别将路由器接口 FastEthernet0/0、FastEthernet0/1 和 FastEthernet1/0 分配给区域 trust、notrust 和 dmz。

```
interface FastEthernet0/0
zone-member security trust
```

进入接口 FastEthernet0/0 配置模式，通过命令 zone—member security trust 将该接口分配给名为 trust 的区域。

```
interface FastEthernet0/1
zone-member security notrust
interface FastEthernet1/0
zone-member security dmz
```

(3) 定义信息流类型。

信任区至非军事区信息流类型：

```
access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7
access-list 112 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3
class-map type inspect match-all trust-dmz-http
match access-group 111
match protocol http
```

class-map type inspect 是用于分类信息流的命令，参数 match-all 表示信息流类型需同时满足以下条件，参数 match-any 表示信息流类型只需满足以下一项条件。trust-dmz-http 是分类的信息流名字。命令 match access-group 111 表示该信息流需符合编号为 111 的访问控制列表，命令 match protocol http 表示该信息流的应用层协议是 http。由于分类信息流命令携带参数 match-all，表示名为 trust-dmz-http 的信息流类型符合编号为 111 的访问控制列表，且应用层协议是 http。

```
class-map type inspect match-all trust-dmz-smtp
match access-group 112
match protocol smtp
```

名为 trust-dmz-smtp 的信息流类型符合编号为 112 的访问控制列表，且应用层协议是 smtp。

```
class-map type inspect match-all trust-dmz-pop3
match access-group 112
match protocol pop3
```

名为 trust-dmz-pop3 的信息流类型符合编号为 112 的访问控制列表，且应用层协议是 pop3。

信任区至非信任区信息流类型：

```
access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7
class-map type inspect match-all trust-notrust
match access-group 121
match protocol http
```

名为 trust-notrust 的信息流类型符合编号为 121 的访问控制列表，且应用层协议是 http。

非军事区至非信任区信息流类型：

```
access-list 131 permit tcp host 192.1.2.3 host 192.1.3.3
class-map type inspect match-all dmz-notrust
match access-group 131
match protocol smtp
```

名为 dmz-notrust 的信息流类型符合编号为 131 的访问控制列表，且应用层协议是 smtp。

非信任区至非军事区信息流类型：

```
access-list 141 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7
access-list 142 permit tcp host 192.1.3.3 host 192.1.2.3
class-map type inspect match-all notrust-dmz-http
match access-group 141
match protocol http
```

名为 notrust-dmz-http 的信息流类型符合编号为 141 的访问控制列表，且应用层协议是 http。

```
class-map type inspect match-all notrust-dmz-smtp
match access-group 142
match protocol smtp
```

名为 notrust-dmz-smtp 的信息流类型符合编号为 142 的访问控制列表，且应用层协议是 smtp。

（4）定义策略。

信任区至非军事区策略

```
policy-map type inspect trust-dmz
class type inspect trust-dmz-http
inspect
class type inspect trust-dmz-smtp
inspect
class type inspect trust-dmz-pop3
inspect
```

policy-map type inspect 是创建策略命令，trust-dmz 是策略名，class type inspect trust-dmz-http 指定信息流是名为 trust-dmz-http 的信息流类型，inspect 是对该信息流施加的操作。

信任区至非信任区策略：

```
policy-map type inspect trust-notrust
class type inspect trust-notrust
inspect
```

非军事区至非信任区策略：

```
policy-map type inspect dmz-notrust
class type inspect dmz-notrust
inspect
```

非信任区至非军事区策略：

```
policy-map type inspect notrust-dmz
class type inspect notrust-dmz-http
inspect
class type inspect notrust-dmz-smtp
inspect
```

（5）将策略作用到区域间信息流。

作用到信任区至非军事区的策略：

```
zone-pair security trust-dmz source trust destination dmz
service-policy type inspect trust-dmz
```

zone-pair security 是确定区域对命令，trust-dmz 是为该区域对定义的名字，source trust 表示源区域是 trust，destination dmz 表示目的区域是 dmz。service-policy type inspect 是作用策略命令，trust-dmz 是策略名。

作用到信任区至非信任区的策略：

```
zone-pair security trust-notrust source trust destination notrust
service-policy type inspect trust-notrust
```

作用到非军事区至非信任区的策略：

```
zone-pair security dmz-notrust source dmz destination notrust
service-policy type inspect dmz-notrust
```

作用到非信任区至非军事区的策略：

```
zone-pair security notrust-dmz source notrust destination dmz
service-policy type inspect notrust-dmz
```

9.2 例题解析

9.2.1 自测题

1. 选择题

(1) 下述________的描述是错误的。

A. 安装杀毒软件的机器是安全的

B. 防火墙具有阻止病毒传播的功能

C. 入侵检测系统具有发现病毒的功能

D. 操作系统漏洞是机器感染病毒的主要原因

(2) 对于防火墙，下述________的描述是错误的。

A. 防火墙主要用于控制网络之间的数据交换过程

B. 防火墙能有效抑制内网终端中的木马外泄信息

C. 防火墙能减缓拒绝服务攻击

D. 防火墙能杜绝病毒从一个网络传播到另一个网络

(3) 对于无状态分组过滤器，下述________的描述是错误的。

A. 无状态分组过滤器用于独立确定每一个 IP 分组是正常转发，还是丢弃

B. 作用于一个方向的无状态分组过滤器只能控制该方向的 IP 分组传输过程

C. 无状态分组过滤器只能检测 IP 首部字段

D. 两个方向上设置的无状态分组过滤器独立控制对应方向上的 IP 分组传输过程

(4) 对于有状态分组过滤器，下述________的描述是错误的。

A. 有状态分组过滤器用于控制基于特定应用的数据交换过程

B. 有状态分组过滤器同时控制两个方向上的 IP 分组传输过程

C. 有状态分组过滤器两个方向上的IP分组传输控制机制存在相互制约

D. 有状态分组过滤器能控制两个特定用户之间的数据交换过程

(5) 对于无状态分组过滤器，下述________的描述是错误的。

A. 能够控制两个不同网络之间的数据传输过程

B. 能够控制两个终端之间的数据传输过程

C. 能够控制两个进程之间的数据传输过程

D. 能够控制一次完整应用所涉及的数据交换过程

(6) 有状态分组过滤器可以对访问过程实施控制，下述________对访问过程的描述是错误的。

A. 访问过程是包括建立、维持和释放的一次完整TCP连接

B. 访问过程是有限时间内两个UDP进程之间的数据传输过程

C. 访问过程是一次完整的Web服务器访问过程

D. 访问过程是一次发送和接收邮件过程

(7) 下述________是有状态分组过滤器和应用层代理之间的主要区别。

A. 检测应用层协议相关信息

B. 对某个应用涉及的完整访问过程实施控制

C. 位于网络间数据传输通路上

D. 实施用户身份鉴别

(8) 下述________有关防火墙的描述是错误的。

A. 用于控制网络间数据交换过程

B. 根据分组的属性和当前会话状态确定正常转发或丢弃分组

C. 能够有效抵御跨网络实施的攻击行为

D. 能够有效监控网络内终端行为

(9) 下述________是有状态分组过滤器和无状态分组过滤器之间的主要区别。

A. 对分组实施的操作有丢弃和正常转发

B. 每一个分组独立地根据与过滤规则的匹配结果确定对其施加的操作

C. 位于网络间数据传输通路上

D. 根据策略控制网络间的数据交换过程

(10) 对于有状态分组过滤器，下述________的描述是错误的。

A. 创建会话时匹配过滤规则

B. 允许属于指定会话的TCP报文传输

C. TCP连接是一次会话过程

D. 配置有状态分组过滤器时静态创建对应会话

2. 填空题

(1) 防火墙的本质是控制________之间的信息交换过程，根据防火墙作用的层次，可以分为________、________和________。事实上目前采用的________已经包含了其他两种防火墙的功能。

(2) 目前常用的分组过滤器分为________和________，它们的主要区别在于

________独立控制每一个 IP 分组的传输过程，而________基于某个应用控制整个数据交换过程。________需要逐个方向设置，________控制整个数据交换过程涉及的两个方向的 IP 分组传输过程。

(3) 无状态分组过滤器可以检测 IP 首部中________、________和________字段，TCP 首部中________、________和________字段，因此可以控制________、________和________之间数据传输过程，甚至通过________控制 TCP 连接发起端。

(4) 如果在某个路由器接口输入方向配置扩展分组过滤器"access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www"，意味着允许正常转发的 IP 分组的源 IP 地址是________，目的 IP 地址是________，源端口号是________，目的端口号是________。

(5) 如果在某个路由器接口输入方向同时配置扩展分组过滤器"access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www"和检测机制"ip inspect name a121 http"，意味着允许建立网络内________的终端发起建立的 TCP 连接，该 TCP 连接两端插口可能是________和________。如果在该路由器接口输出方向配置扩展分组过滤器"access-list 112 deny ip any any"，该路由器接口输出方向________输出 IP 分组，但只能输出________的 IP 分组。对应于前面建立的 TCP 连接，允许输出的 IP 分组的协议字段是________，源 IP 地址是________，目的 IP 地址是________。

(6) 堡垒主机一是________，其________和________具有非常好的安全性；二是________，只安装________或________，不会安装普通用户软件。

3. 名词解释

____应用层网关　　　　____访问控制列表
____防火墙　　　　____有状态分组过滤器
____堡垒主机　　　　____个人防火墙
____无状态分组过滤器　　　　____电路层网关

(a) 一种用于对网络间数据交换过程实施控制的设备。

(b) 一种根据会话状态和 IP 分组属性确定正常转发或丢弃 IP 分组的防火墙。

(c) 一种将每一个 IP 分组作为独立个体，并根据 IP 分组属性确定正常转发或丢弃 IP 分组的防火墙。

(d) 一种作为两端之间 TCP 连接的中继设备，并能够对发起 TCP 连接的一方实施身份鉴别的防火墙。

(e) 一种作为客户端和服务器端之间的中继设备，并能够对客户端实施身份鉴别的防火墙。

(f) Cisco 对无状态分组过滤器的称呼。

(g) 一种常作为电路层网关和应用层网关平台，其硬件结构和系统软件有着非常好的安全性的主机。

(h) 一个对进出主机的 IP 分组实施控制的系统进程。

4. 判断题

(1) 分组过滤器可以正常转发或丢弃两个特定终端之间传输的分组。

（2）分组过滤器可以正常转发或丢弃两个特定用户之间传输的分组。

（3）电路层网关可以正常转发或丢弃两个特定用户之间传输的 TCP 报文。

（4）有状态分组过滤器是实现防火墙功能的一种技术。

（5）防火墙本身是一个可信系统。

（6）堡垒主机是一种安装应用层网关软件的普通主机系统。

（7）有状态分组过滤器创建会话的前提是扩展分组过滤器允许该 IP 分组正常转发，且该 IP 分组净荷是检测机制指定的应用层或传输层协议的协议数据单元。

（8）如果某个 IP 分组和有状态分组过滤器已经建立的某个会话匹配，则直接转发该 IP 分组。

（9）如果用防火墙对网络间数据交换过程实施控制，则网络间数据传输通路必须经过防火墙。

（10）有状态分组过滤器对两端是透明的。

（11）电路层网关和应用层网关对两端通常是不透明的。

9.2.2　自测题答案

1. 选择题答案

（1）A，一般情况下杀毒软件无法防止未知病毒。

（2）D，防火墙的主要功能是控制网络间数据交换过程，检测数据中是否携带病毒不是防火墙的主要任务，杜绝病毒传播更是不可能。

（3）C，不但检测 IP 首部，还检测传输层首部。

（4）D，有状态分组过滤器不具有身份鉴别功能，无法确定数据的发送和接收用户。

（5）D，这是有状态分组过滤器才具有的功能。

（6）D，发送邮件和接收邮件是两个独立的访问过程。

（7）D，这是应用层网关具备，有状态分组过滤器不具备的功能。

（8）D，防火墙只能对网络间传输的数据实施控制，一般无法监控网络内的信息流模式。

（9）B，这是无状态分组过滤器的特性。

（10）D，会话是动态创建的，当扩展分组过滤器允许某个 IP 分组正常转发，且该 IP 分组净荷是检测机制指定的应用层或传输层协议的协议数据单元时，创建会话。

2. 填空题答案

（1）网络，分组过滤器，电路层网关，应用层网关，有状态分组过滤器。

（2）无状态分组过滤器，有状态分组过滤器，无状态分组过滤器，有状态分组过滤器，无状态分组过滤器，有状态分组过滤器。

（3）源 IP 地址，目的 IP 地址，协议，源端口号，目的端口号，控制位，网络，终端，进程，ACK 控制位。

（4）属于网络地址 192.1.1.0/24，192.1.2.7，任意，80。

（5）192.1.1.0/24，192.1.1.1:2345，192.1.2.7:80，允许，属于由两端插口 192.1.1.1:2345 和 192.1.2.7:80 标识的 TCP 连接，TCP，192.1.2.7，192.1.1.1。

(6) 可信系统,硬件结构,系统软件,专用系统,电路层网关软件,应用层网关软件。

3. 名词解释答案

e 应用层网关	f 访问控制列表
a 防火墙	b 有状态分组过滤器
g 堡垒主机	h 个人防火墙
c 无状态分组过滤器	d 电路层网关

4. 判断题答案

(1) 对,基于源和目的 IP 地址可以确定发送和接收终端。

(2) 错,基于用户控制,首先需要鉴别用户身份,然后绑定用户和 IP 地址之间关系,分组过滤器没有鉴别用户身份功能。

(3) 对,一是电路层网关在传输层实施控制,二是电路层网关具有鉴别用户身份功能。

(4) 对,有状态分组过滤器实现的是防火墙的功能。

(5) 对,否则,黑客首先入侵防火墙。

(6) 错,堡垒主机一是可信系统,二是专用系统,即在安全平台上只安装电路层或应用层网关软件的主机。

(7) 对,如果某个 IP 分组不属于已经建立的会话,且扩展分组过滤器允许该 IP 分组正常转发,创建对应会话。

(8) 对,如果某个 IP 分组属于某个已经建立的会话,无须匹配扩展分组过滤器,直接转发。

(9) 对,否则,可以绕过防火墙,防火墙形同虚设。

(10) 对,两端数据交换过程中感觉不到有状态分组过滤器的存在。

(11) 对,发起端需要给出作为代理的电路层网关或应用层网关的 IP 地址。

9.2.3 简答题解析

1. 简述无状态分组过滤器控制网络间数据传输的过程。

回答: 通过定义分组过滤器配置一组规则,规则指定了正常转发和丢弃的 IP 分组类型,将分组过滤器作用于路由器接口的输入或输出方向,一旦某个 IP 分组需要从该路由器接口输入或输出,依照顺序和分组过滤器中的规则逐个匹配,一旦和某个规则匹配,对该 IP 分组施加规则指定的操作。

2. 简述有状态分组过滤器控制网络间数据传输的过程。

回答: 一般需要定义分组过滤器和检测机制,然后将分组过滤器和检测机制作用于路由器接口的输入或输出方向,一旦某个 IP 分组需要从该路由器接口输入或输出,首先和该路由器已经建立的会话匹配,如果该 IP 分组和某个已经建立的会话匹配,直接转发该 IP 分组,否则和同方向的分组过滤器进行匹配操作,一旦匹配的结果是允许正常转发,且该 IP 分组净荷是检测机制指定的传输层或应用层协议的协议数据单元,创建对应会话。会话通常是用于传输应用层报文的 TCP 连接,当然也可以是两个 UDP 进程之间的数据交换过程,或是 ICMP 的一次请求、响应过程。和无状态分组过滤器不同,一是只有

在该 IP 分组没有和路由器已经建立的会话匹配的情况下，才需要和该 IP 分组相同传输方向的分组过滤器进行匹配操作，并对该 IP 分组施加匹配规则指定的操作。二是一旦该 IP 分组与相同传输方向的分组过滤器匹配操作的结果是正常转发，且该 IP 分组净荷是检测机制指定的传输层或应用层协议的协议数据单元，创建对应会话，以后两个传输方向所有属于该会话的 IP 分组直接转发，这些 IP 分组的转发操作与两个方向配置的分组过滤器无关。

3. 简述两个特定终端之间传输的 IP 分组和两个特定用户之间传输的 IP 分组的区别。

回答：为了确定某个 IP 分组的发送和接收用户，首先需要鉴别用户身份，在鉴别用户身份过程中建立该用户与 IP 地址之间的绑定关系，这种绑定关系是动态的，因为同一用户可以通过不同的终端发送和接收数据。在该用户与 IP 地址之间的绑定关系存在期间，可以通过检测源和目的 IP 地址是否是该用户绑定的 IP 地址来确定该 IP 分组是否由该用户发送或接收。为了防止源 IP 地址欺骗，有时需要通过安全协议 AH 来保证 IP 分组传输过程中的完整性。

9.2.4　综合题解析

1. 如果某个路由器接口输入方向配置编号为 101 的扩展分组过滤器，输出方向配置编号为 102 的扩展分组过滤器，同时在输入方向配置名为 a101 的检测机制。如果顺序传输下列 IP 分组，给出路由器完成的操作。

```
access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www
access-list 101 permit icmp host 192.1.1.1 host 192.1.2.7
access-list 102 permit icmp host 192.1.2.7 host 192.1.1.1
ip inspect name a101 tcp
```

① 输出，协议＝TCP，源 IP 地址＝192.1.2.7，目的 IP 地址＝192.1.1.1，源端口号＝80，目的端口号＝1234；

② 输出，协议＝ICMP，源 IP 地址＝192.1.2.7，目的 IP 地址＝192.1.1.1；

③ 输入，协议＝TCP，源 IP 地址＝192.1.1.1，目的 IP 地址＝192.1.2.7，源端口号＝1234，目的端口号＝80；

④ 输出，协议＝TCP，源 IP 地址＝192.1.2.7，目的 IP 地址＝192.1.1.1，源端口号＝80，目的端口号＝1234；

⑤ 输出，协议＝TCP，源 IP 地址＝192.1.2.7，目的 IP 地址＝192.1.1.1，源端口号＝80，目的端口号＝4321；

⑥ 输入，协议＝TCP，源 IP 地址＝192.1.1.1，目的 IP 地址＝192.1.2.7，源端口号＝80，目的端口号＝1234。

解析：① 由于路由器已经建立的会话为空，该 IP 分组与输出方向的扩展分组过滤器进行匹配操作，由于不存在和该 IP 分组匹配的规则，丢弃该 IP 分组。

② 由于路由器已经建立的会话为空，该 IP 分组与输出方向的扩展分组过滤器进行匹配操作，由于与规则 permit icmp host 192.1.2.7 host 192.1.1.1 匹配，实施规则指定

操作：正常转发。由于输出方向没有配置检测机制，因此路由器只是正常转发该 IP 分组，不创建会话。

③ 由于路由器已经建立的会话为空，该 IP 分组与输入方向的扩展分组过滤器进行匹配操作，由于与规则 permit tcp host 192.1.1.1 host 192.1.2.7 eq www 匹配，实施规则指定操作：正常转发。由于输入方向配置检测机制，且检测机制指定的传输层协议是 TCP，与 IP 分组净荷一致，因此创建会话，会话是两端插口分别是 192.1.1.1:1234 和 192.1.2.7:80 的 TCP 连接。

④ 由于路由器已经建立会话，该 IP 分组首先与已经建立的会话进行匹配操作，由于该 IP 分组属于两端插口分别是 192.1.1.1:1234 和 192.1.2.7:80 的 TCP 连接，直接转发该 IP 分组，无需与输出方向的扩展分组过滤器进行匹配操作。

⑤ 由于路由器已经建立会话，该 IP 分组首先与已经建立的会话进行匹配操作，但该 IP 分组不属于已经建立的 TCP 连接，需要与输出方向的扩展分组过滤器进行匹配操作，匹配操作结果是丢弃该 IP 分组。

⑥ 该 IP 分组不属于已经建立的 TCP 连接，和输入方向扩展分组过滤器的匹配操作结果是丢弃。

2. 如果某个路由器接口输入方向配置编号为 101 的扩展分组过滤器，输出方向配置编号为 102 的扩展分组过滤器，同时在输入方向配置名为 a101 的检测机制。如果顺序传输下列 IP 分组，给出路由器完成的操作。

```
access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7
access-list 101 permit icmp host 192.1.1.1 host 192.1.2.7
access-list 102 deny ip any any
ip inspect name a101 tcp
ip inspect name a101 icmp
```

① 输出，协议=TCP，源 IP 地址=192.1.2.7，目的 IP 地址=192.1.1.1，源端口号=80，目的端口号=1234。

② 输出，协议=ICMP，源 IP 地址=192.1.2.7，目的 IP 地址=192.1.1.1，ECHO 响应。

③ 输入，协议=TCP，源 IP 地址=192.1.1.1，目的 IP 地址=192.1.2.7，源端口号=1234，目的端口号=80。

④ 输出，协议=TCP，源 IP 地址=192.1.2.7，目的 IP 地址=192.1.1.1，源端口号=80，目的端口号=1234。

⑤ 输入，协议=ICMP，源 IP 地址=192.1.1.1，目的 IP 地址=192.1.2.7，ECHO 请求。

⑥ 输入，协议=TCP，源 IP 地址=192.1.1.1，目的 IP 地址=192.1.2.7，源端口号=80，目的端口号=1234。

⑦ 输出，协议=ICMP，源 IP 地址=192.1.2.7，目的 IP 地址=192.1.1.1，ECHO 响应。

解析：① 由于路由器已经建立的会话为空，且输出方向扩展分组过滤器禁止一切 IP 分组转发，丢弃该 IP 分组。

② 丢弃该 IP 分组，原因和①相同。

③ 转发该 IP 分组，建立两端插口分别是 192.1.1.1:1234 和 192.1.2.7:80 的 TCP 连接。

④ 属于已经建立的 TCP 连接，直接转发该 IP 分组。

⑤ 转发该 IP 分组，创建会话，会话是 IP 地址为 192.1.1.1 与 IP 地址为 192.1.2.1 的两个终端之间的 ICMP ECHO 请求、响应过程。

⑥ 由于输入方向扩展分组过滤器没有目的端口号限制，匹配结果是正常转发该 IP 分组，同时建立两端插口分别是 192.1.1.1:80 和 192.1.2.7:1234 的 TCP 连接。

⑦ 该 IP 分组属于 IP 地址为 192.1.1.1 与 IP 地址为 192.1.2.1 的两个终端之间的 ICMP ECHO 请求、响应过程，直接转发。由于该 ICMP ECHO 请求、响应过程完成，删除该会话。

9.3 实　验

9.3.1 标准分组过滤器配置实验

1. 实验内容

(1) 配置标准分组过滤器。

(2) 验证标准分组过滤器的单向控制功能。

(3) 验证网络间分组传输控制过程。

2. 网络结构

网络结构如图 9.3 所示。要求禁止终端 A 发送的 IP 分组离开网络 192.1.1.0/24，终端 C 发送的 IP 分组离开网络 192.1.2.0/24。但允许终端 D 发送的 IP 分组到达终端 A，终端 B 发送的 IP 分组到达终端 C。

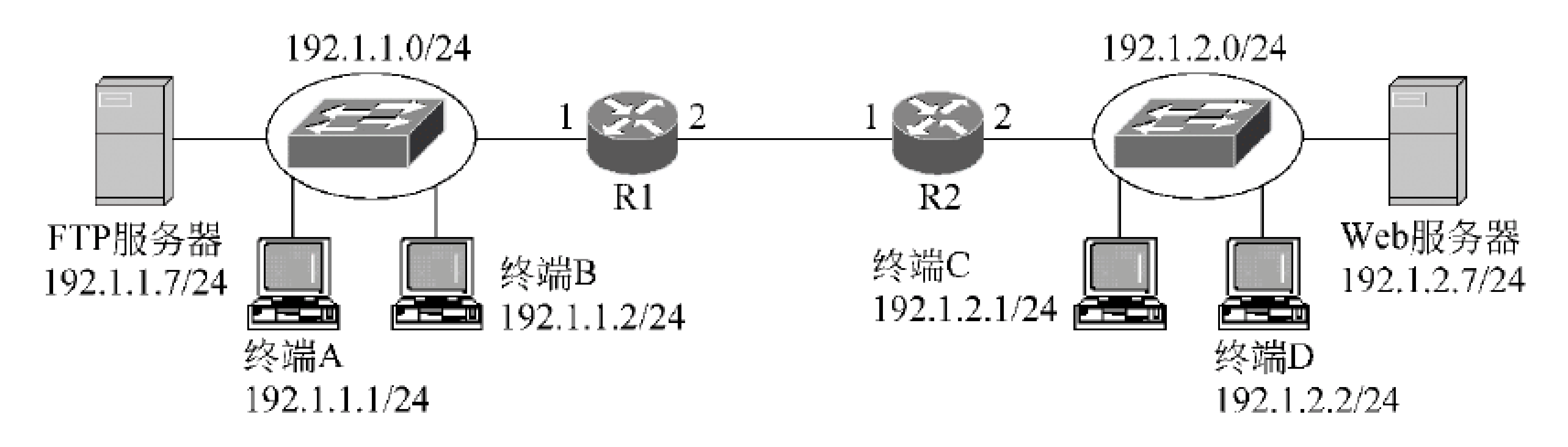


图 9.3　配置标准和扩展分组过滤器网络结构

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 9.3 所示的网络结构放置和连接设备，逻辑工作区完成设备放置和连接后的界面如图 9.4 所示。

(2) 完成路由器 Router0 和 Router1 接口 IP 地址和子网掩码配置，启动 RIP 进程，建立动态路由项。完成终端和服务器 IP 地址和子网掩码配置，其中 PC0、PC1、PC2 和 PC3 分别配置 IP 地址和子网掩码 192.1.1.1/24、192.1.1.2/24、192.1.2.1/24 和 192.1.2.2/24。完成配置后，Router0 和 Router1 生成图 9.4 所示路由表。验证终端、服务器之间的相互通信功能。

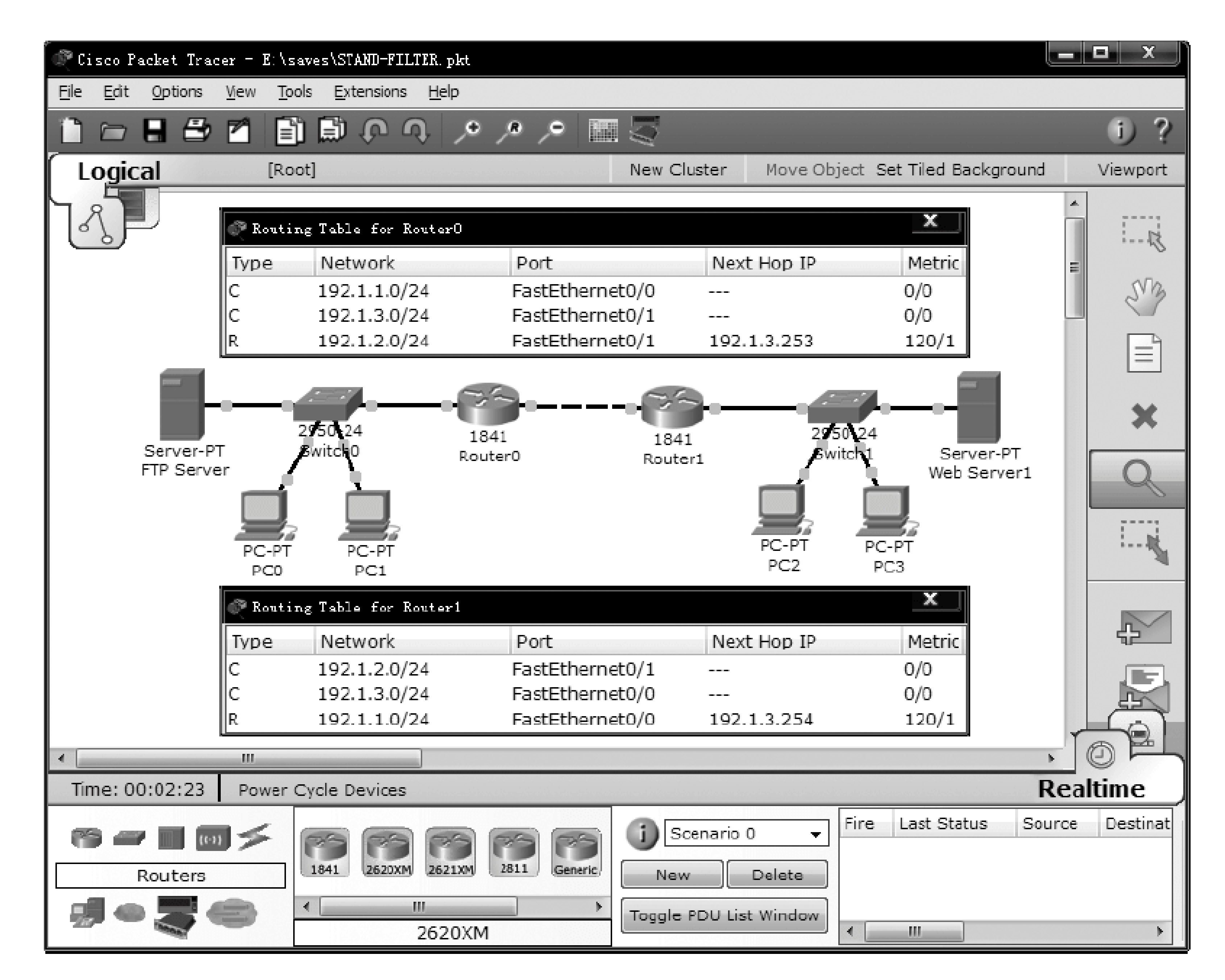


图 9.4 放置和连接设备后的逻辑工作区界面及路由表

(3) 定义拒绝源 IP 地址为 192.1.1.1/32 的 IP 分组的标准分组过滤器，并将其作用于路由器 Router0 接口 FastEthernet0/0 的输入方向。定义拒绝源 IP 地址为 192.1.2.1/32 的 IP 分组的标准分组过滤器，并将其作用于路由器 Router1 接口 FastEthernet0/1 的输入方向。

(4) 通过 Ping 操作验证 PC0 和 PC2 无法和其他网络中的终端交换分组。

(5) 进入模拟操作模式，验证 PC1 至 PC2，PC3 至 PC0 的单向通信功能。用户定义的 PC1 至 PC2 的分组格式如图 9.5 所示。

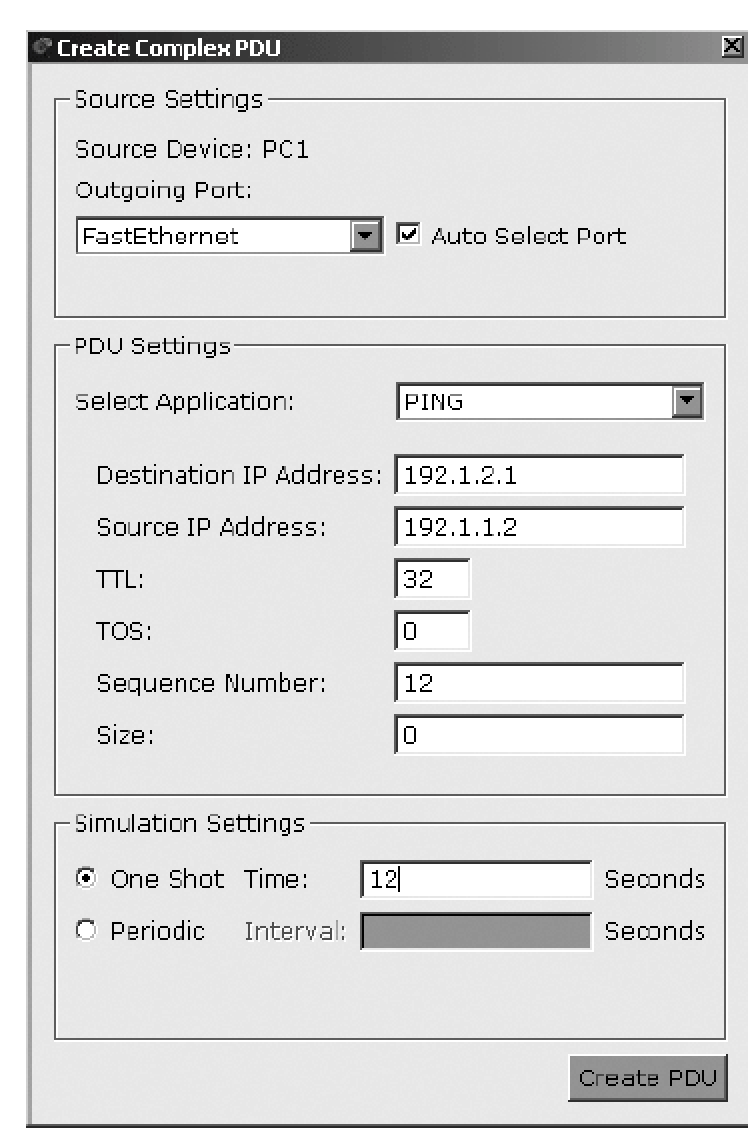


图 9.5 实现 PC1 至 PC2 单向通信功能的 IP 分组

4. 路由器命令行配置过程

(1) Router0 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.254 255.255.
255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.254 255.255.
```

```
255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.1.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#access-list 1 deny 192.1.1.1 0.0.0.0
```

(定义标准分组过滤器的一个过滤规则,1 是编号,标准分组过滤器的编号范围为 1~99,属于同一分组过滤器的过滤规则必须具有相同的编号。该过滤规则拒绝转发源 IP 地址为 192.1.1.1/32 的 IP 分组。0.0.0.0 的作用相当于是子网掩码的反码,IP 分组源 IP 地址中 0 对应的位数需要和过滤规则中给出的 IP 地址比较,1 对应的位数不需要比较。192.1.1.1 0.0.0.0 可以用 host 192.1.1.1 代替)

```
Router(config)#access-list 1 permit any
```

(该过滤规则允许所有 IP 分组正常转发,一旦定义分组过滤器,最后一项是隐含的、拒绝所有 IP 分组正常转发的过滤规则。因此,如果仅仅拒绝一部分 IP 分组正常转发,需要给出允许其他 IP 分组正常转发的过滤规则。any 等同于 0.0.0.0 255.255.255.255)

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 1 in
```

(将编号为 1 的标准分组过滤器作用于接口 FastEthernet0/0 输入方向,in 表示输入方向)

```
Router(config-if)#exi
Router(config)#
```

(2) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.253 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.3.0
Router(config-router)#exit
Router(config)#access-list 1 deny 192.1.2.1 0.0.0.0
Router(config)#access-list 1 permit any
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#
```

9.3.2 扩展分组过滤器配置实验

1. 实验内容

(1) 配置扩展分组过滤器。

(2) 验证扩展分组过滤器的单向控制功能。

(3) 验证网络间分组传输控制过程。

2. 网络结构

网络结构如图 9.3 所示。要求实现只允许终端 A 发起访问 Web 服务器,终端 B 发起访问 FTP 服务器,禁止其他一切网络间通信的数据传输控制。

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 9.3 所示的网络结构放置和连接设备,逻辑工作区完成设备放置和连接后的界面如图 9.4 所示。

(2) 完成路由器 Router0 和 Router1 以及终端和服务器的配置。路由器 Router0 和 Router1 路由表如图 9.4 所示。验证终端、服务器之间的相互通信功能。

(3) 定义作用于路由器 Router0 接口 FastEthernet0/0 输入方向的扩展分组过滤器,扩展分组过滤器中包含的过滤规则保证只允许 FTP 服务器至 PC2 的 TCP 报文和 PC0 至 Web 服务器的 TCP 报文正常转发,拒绝其他 IP 分组。定义作用于路由器 Router1 接口 FastEthernet0/1 输入方向的扩展分组过滤器,分组过滤器中包含的过滤规则保证只允许 Web 服务器至 PC0 的 TCP 报文和 PC2 至 FTP 服务器的 TCP 报文正常转发,拒绝其他 IP 分组。

(4) 验证网络拒绝所有通过 Ping 操作进行的网络间通信过程。

(5) 验证 PC0 访问 Web 服务器过程。图 9.6 给出 PC0 通过实用程序 Web Browser

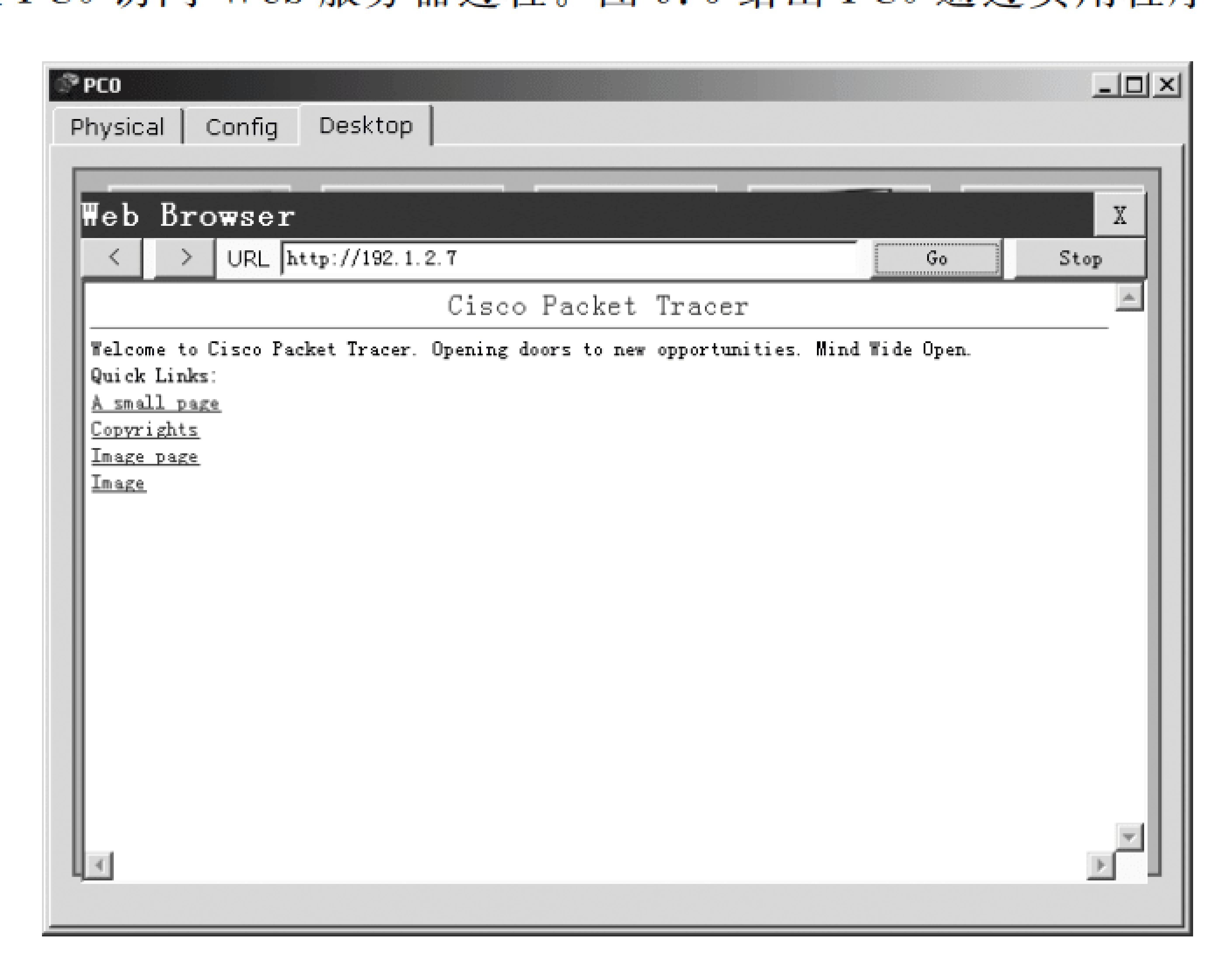


图 9.6 PC0 成功访问 Web 服务器界面

访问 Web 服务器的界面，验证 PC2 访问 FTP 服务器过程。图 9.7 给出 PC2 通过命令行接口访问 FTP 服务器的界面。

（6）进入模拟操作模式，创建图 9.8 所示的 Web 服务器用 Telnet 访问 PC0 的 TCP 报文，将 TCP 报文的源端口号设置为 80，结果发现该 TCP 报文能够顺利到达 PC0，表明扩展分组过滤器其实并没有真正实现只允许终端 A 发起访问 Web 服务器，终端 B 发起访问 FTP 服务器，禁止其他一切网络间通信的数据传输控制。

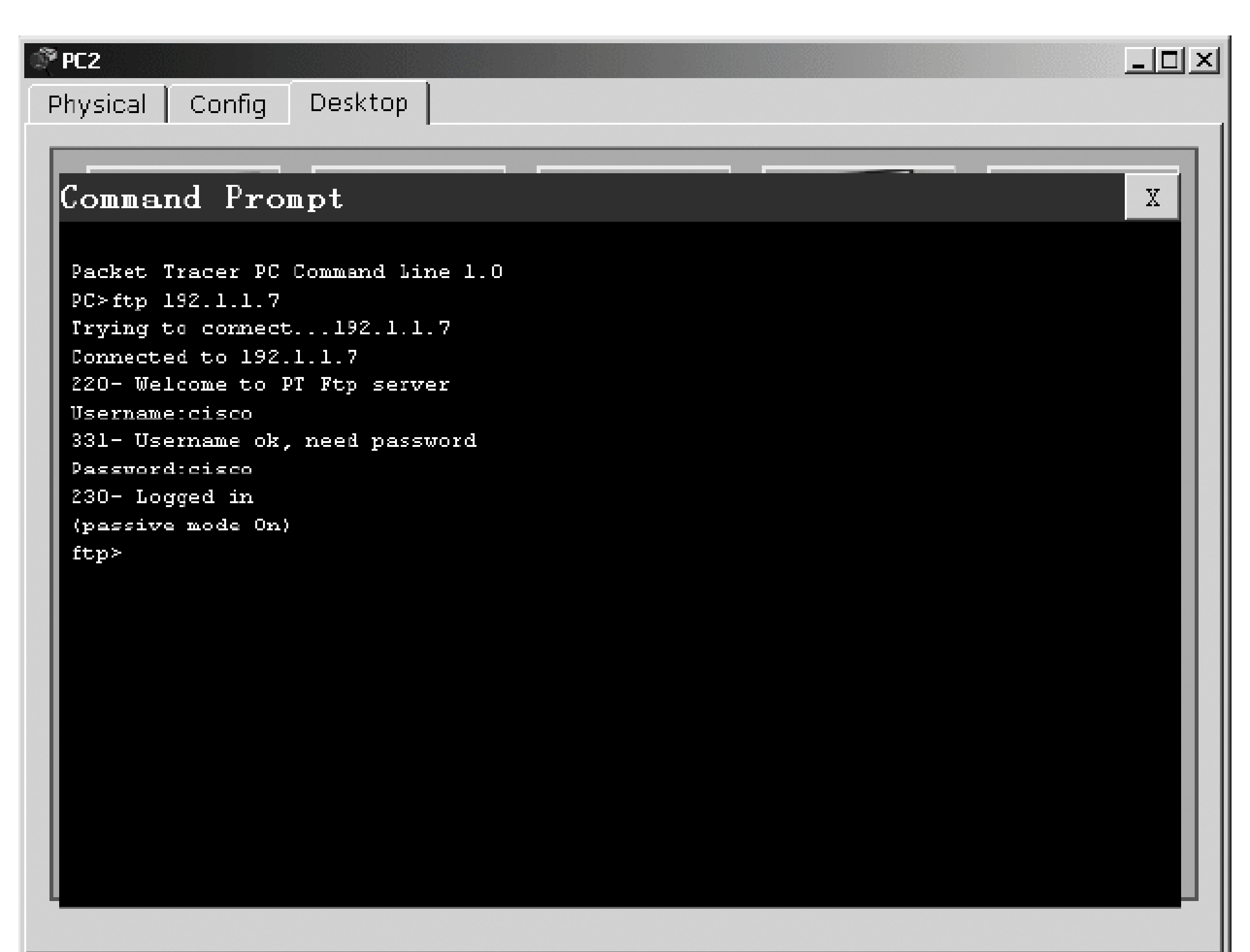


图 9.7 PC2 成功访问 FTP 服务器界面

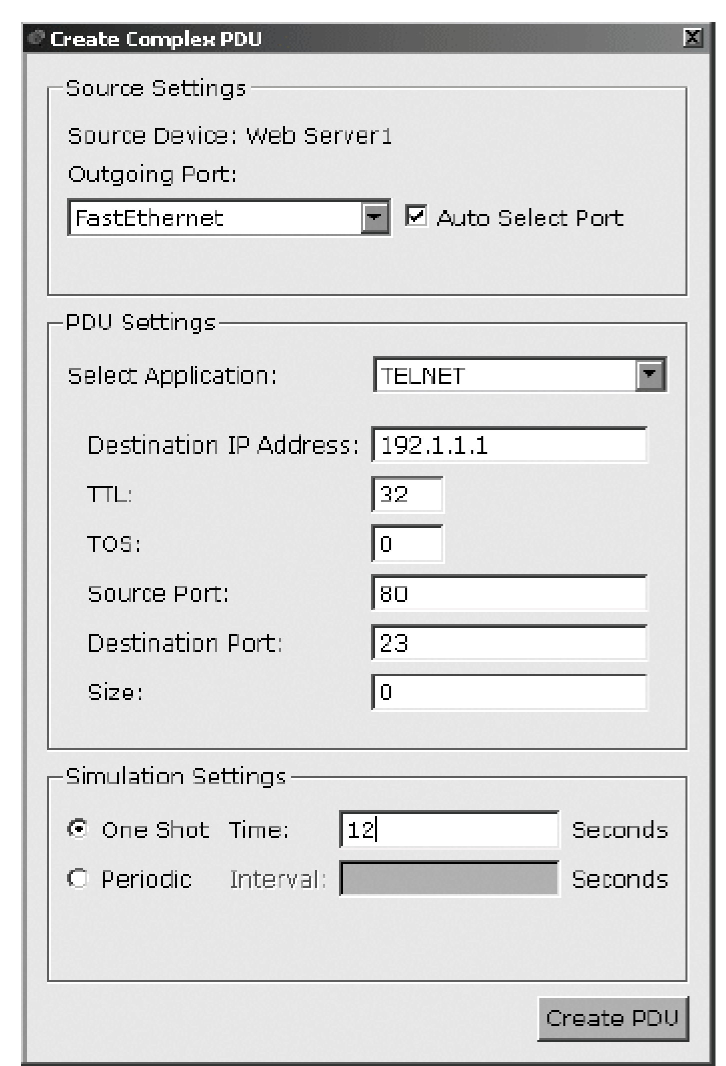


图 9.8 实现 Web 服务器至 PC0 单向通信的 Telnet 报文

4. 命令行配置过程

（1）Router0 分组过滤器部分命令行配置过程。

Router(config)#access-list 101 permit tcp 192.1.1.1 0.0.0.0 192.1.2.7 0.0.0.0 eq 80

（编号 100~199 表明是扩展分组过滤器，该过滤规则表明允许源 IP 地址=192.1.1.1/32，源端口号任意，目的 IP 地址=192.1.2.7/32，目的端口号=80 的 TCP 报文正常转发。192.1.1.1 0.0.0.0 可以用 host 192.1.1.1 代替，192.1.2.7 0.0.0.0 可以用 host 192.1.2.7 代替）

Router(config)#access-list 101 permit tcp 192.1.1.7 0.0.0.0 eq 20 192.1.2.1 0.0.0.0

（该过滤规则表明允许源 IP 地址=192.1.1.7/32，源端口号=20，目的 IP 地址=192.1.2.1/32，目的端口号任意的 TCP 报文正常转发。属于同一分组过滤器的过滤规则必须具有相同的编号）

Router(config)#access-list 101 permit tcp 192.1.1.7 0.0.0.0 eq 21 192.1.2.1 0.0.0.0

（该过滤规则表明允许源 IP 地址=192.1.1.7/32，源端口号=21，目的 IP 地址=192.1.2.1/32，目的端口号任意的 TCP 报文正常转发）

Router(config)#access-list 101 deny ip any any （该过滤规则拒绝其他一切 IP 分组）

Router(config)#interface FastEthernet0/0

Router(config-if)#ip access-group 101 in

(将编号为 101 的扩展分组过滤器作用于接口 FastEthernet0/0 输入方向)

Router(config-if)#exit

(下面是实现相同功能的另一种命令行配置过程。先用命令"ip access-list extended a1"定义一个名为 a1 的扩展分组过滤器,然后在该扩展分组过滤器的配置过程中输入所有属于该扩展分组过滤器的过滤规则)

Router(config)#ip access-list extended a1 (创建名为 a1 的扩展分组过滤器)

Router(config-ext-nacl)#permit tcp 192.1.1.1 0.0.0.0 192.1.2.7 0.0.0.0 eq 80

Router(config-ext-nacl)#permit tcp 192.1.1.7 0.0.0.0 eq 20 192.1.2.1 0.0.0.0

Router(config-ext-nacl)#permit tcp 192.1.1.7 0.0.0.0 eq 21 192.1.2.1 0.0.0.0

Router(config-ext-nacl)#deny ip any any

Router(config-ext-nacl)#exit

Router(config)#interface FastEthernet0/0

Router(config-if)#ip access-group a1 in

(将名为 a1 的扩展分组过滤器作用于接口 FastEthernet0/0 输入方向)

Router(config-if)#exit

(2) Router1 分组过滤器部分命令行配置过程。

Router(config)#access-list 101 permit tcp 192.1.2.7 0.0.0.0 eq 80 192.1.1.1 0.0.0.0

(该过滤规则表明允许源 IP 地址=192.1.2.7/32,源端口号=80,目的 IP 地址=192.1.1.1/32,目的端口号任意的 TCP 报文正常转发)

Router(config)#access-list 101 permit tcp 192.1.2.1 0.0.0.0 192.1.1.7 0.0.0.0 eq 20

(该过滤规则表明允许源 IP 地址=192.1.2.1/32,源端口号任意,目的 IP 地址=192.1.1.7/32,目的端口号=20 的 TCP 报文正常转发)

Router(config)#access-list 101 permit tcp 192.1.2.1 0.0.0.0 192.1.1.7 0.0.0.0 eq 21

(该过滤规则表明允许源 IP 地址=192.1.2.1/32,源端口号任意,目的 IP 地址=192.1.1.7/32,目的端口号=21 的 TCP 报文正常转发)

Router(config)#access-list 101 deny ip any any (该过滤规则拒绝其他一切 IP 分组)

Router(config)#interface FastEthernet0/1

Router(config-if)#ip access-group 101 in

(将编号为 101 的扩展分组过滤器作用于接口 FastEthernet0/1 输入方向)

Router(config-if)#exit

(下面是实现相同功能的另一种命令行配置过程。先用命令 ip access-list extended a1 定义一个名为 a1 的扩展分组过滤器,然后在该扩展分组过滤器的配置过程中输入所有属于该扩展分组过滤器的过滤规则)

Router(config)#ip access-list extended a1

Router(config-ext-nacl)#permit tcp 192.1.2.7 0.0.0.0 eq 80 192.1.1.1 0.0.0.0

Router(config-ext-nacl)#permit tcp 192.1.2.1 0.0.0.0 192.1.1.7 0.0.0.0 eq 20

Router(config-ext-nacl)#permit tcp 192.1.2.1 0.0.0.0 192.1.1.7 0.0.0.0 eq 21

Router(config-ext-nacl)#deny ip any any

Router(config-ext-nacl)#exit

Router(config)#

Router(config)#interface FastEthernet0/1

Router(config-if)#ip access-group a1 in

(将名为 a1 的扩展分组过滤器作用于接口 FastEthernet0/1 输入方向)

```
Router(config-if)#exit
```

9.3.3　有状态分组过滤器配置实验

1. 实验内容

(1) 配置有状态分组过滤器。

(2) 验证有状态分组过滤器的双向控制功能。

(3) 验证网络间分组传输控制过程。

2. 网络结构

网络结构如图 9.9 所示。要求配置实现满足下列访问控制策略的 Cisco 有状态分组过滤器。

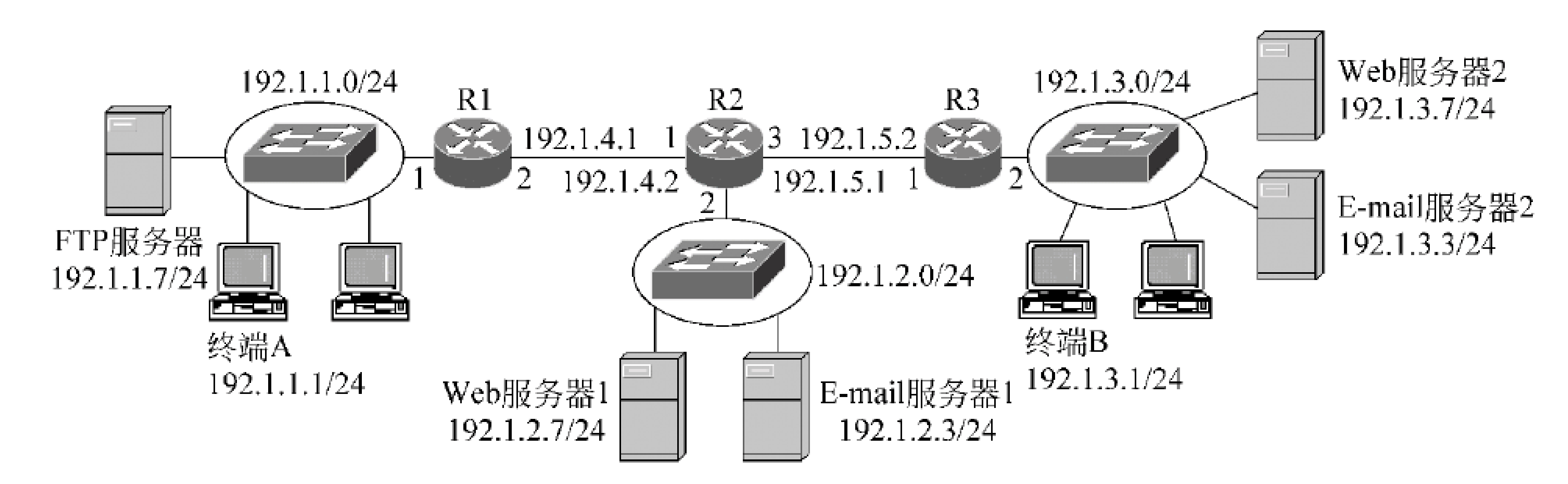


图 9.9　配置 Cisco 有状态分组过滤器的网络结构

① 允许网络 192.1.1.0/24 中的终端访问 Web 服务器 1。

② 允许网络 192.1.1.0/24 中的终端访问 E-mail 服务器 1(SMTP+POP3)。

③ 允许网络 192.1.1.0/24 中的终端访问 Web 服务器 2。

④ 允许 E-mail 服务器 1 访问 E-mail 服务器 2(SMTP)。

⑤ 允许网络 192.1.3.0/24 中的终端访问 Web 服务器 1。

⑥ 允许 E-mail 服务器 2 访问 E-mail 服务器 1(SMTP)。

⑦ 禁止其他一切数据交换过程。

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 9.9 所示的网络结构放置和连接设备，逻辑工作区完成设备放置和连接后的界面如图 9.10 所示。

(2) 根据图 9.9 所示的配置信息完成路由器 Router1、Router2 和 Router3 接口 IP 地址和子网掩码配置，在各个路由器中启动 RIP 进程，配置参与建立动态路由项的网络地址和接口，路由器 Router1、Router2 和 Router3 生成图 9.11～图 9.13 所示的路由表。根据图 9.9 所示的配置信息完成终端和服务器的 IP 地址和子网掩码配置。验证终端、服务器之间的相互通信功能。

(3) 由 Router2 实施访问控制策略。对于访问控制策略允许的访问过程，访问控制列表允许与访问过程相关的 TCP 报文沿着发起访问的传输方向继续传输，但在同方向配置检测该访问过程相关的应用层协议的检测机制。相反方向通过配置访问控制列表拒绝任何

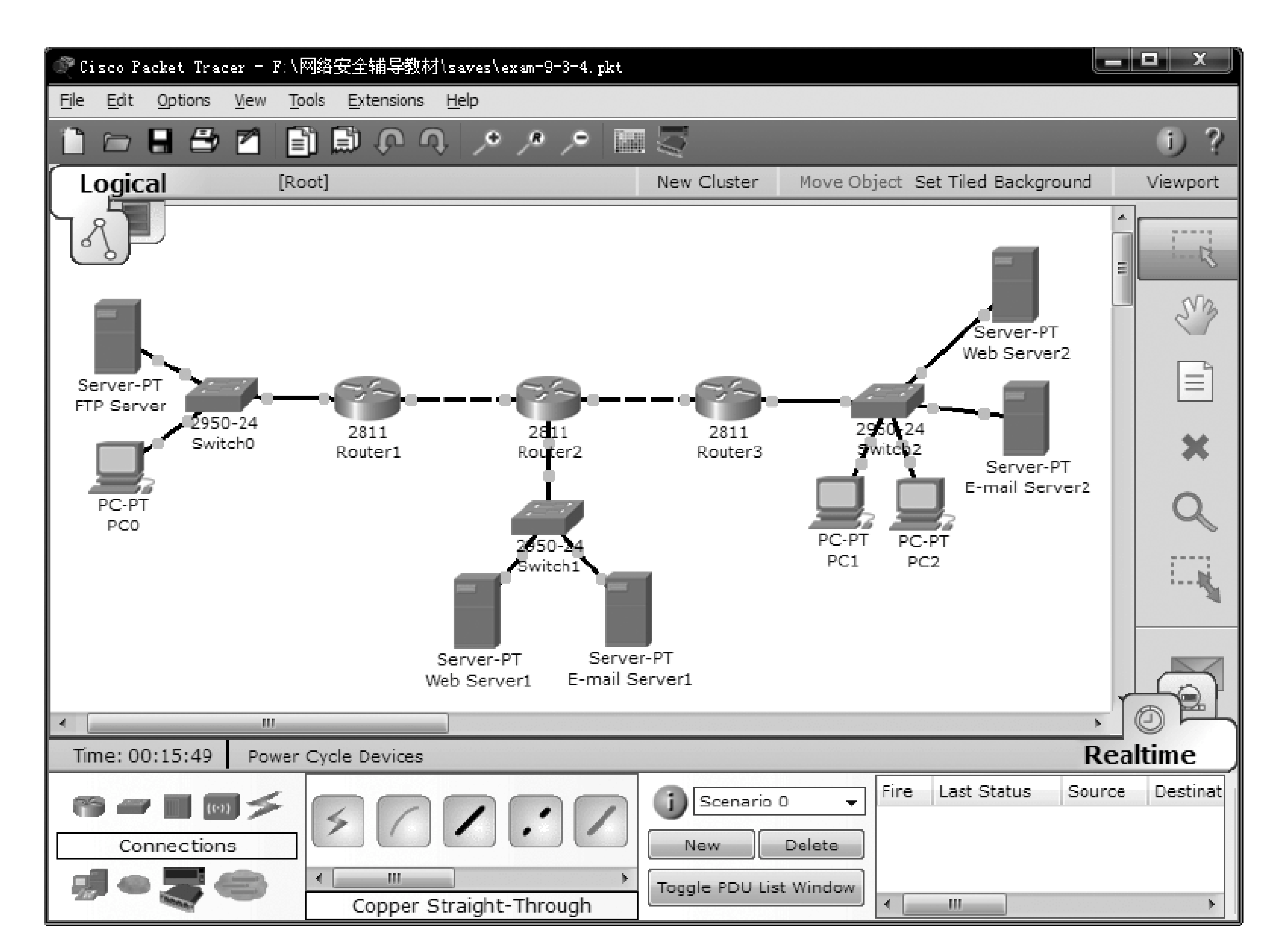
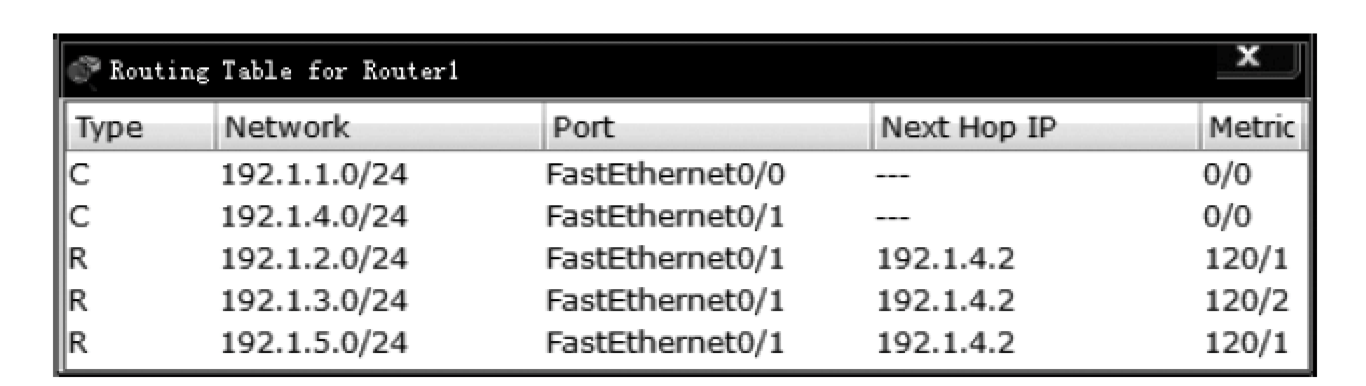
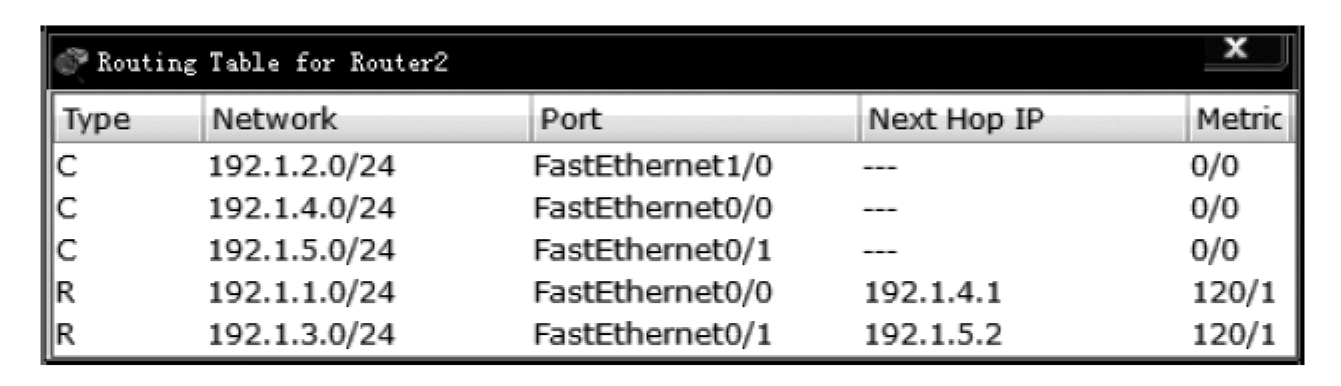


图 9.10 放置和连接设备后的逻辑工作区界面


Routing Table for Router1

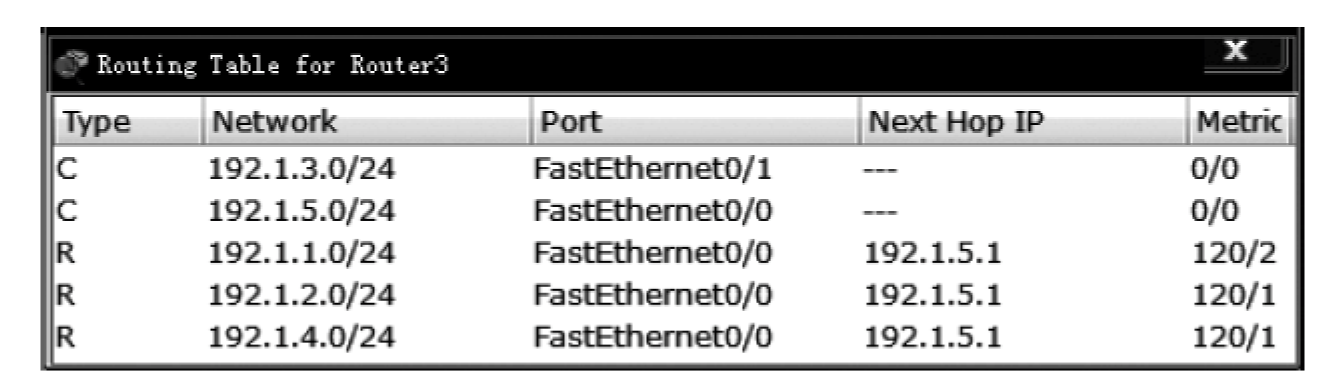
Type	Network	Port	Next Hop IP	Metric
C	192.1.1.0/24	FastEthernet0/0	---	0/0
C	192.1.4.0/24	FastEthernet0/1	---	0/0
R	192.1.2.0/24	FastEthernet0/1	192.1.4.2	120/1
R	192.1.3.0/24	FastEthernet0/1	192.1.4.2	120/2
R	192.1.5.0/24	FastEthernet0/1	192.1.4.2	120/1

图 9.11 Router1 路由表


Routing Table for Router2

Type	Network	Port	Next Hop IP	Metric
C	192.1.2.0/24	FastEthernet1/0	---	0/0
C	192.1.4.0/24	FastEthernet0/0	---	0/0
C	192.1.5.0/24	FastEthernet0/1	---	0/0
R	192.1.1.0/24	FastEthernet0/0	192.1.4.1	120/1
R	192.1.3.0/24	FastEthernet0/1	192.1.5.2	120/1

图 9.12 Router2 路由表


Routing Table for Router3

Type	Network	Port	Next Hop IP	Metric
C	192.1.3.0/24	FastEthernet0/1	---	0/0
C	192.1.5.0/24	FastEthernet0/0	---	0/0
R	192.1.1.0/24	FastEthernet0/0	192.1.5.1	120/2
R	192.1.2.0/24	FastEthernet0/0	192.1.5.1	120/1
R	192.1.4.0/24	FastEthernet0/0	192.1.5.1	120/1

图 9.13 Router3 路由表

TCP 报文传输。Router2 有状态分组过滤器配置过程参见 9.1.2 节中有关 Cisco 有状态分组过滤器配置实例这一部分。

(4) 验证实现访问控制策略的有状态分组过滤器配置,图 9.14 是 PC0 成功访问 Web Server1 的界面。可以通过 PC0 成功访问 Web Server2 和 PC1 成功访问 Web Server1 验证允许属于网络 192.1.1.0/24 的终端访问 Web Server1 和 Web Server2,允许属于网络 192.1.3.0/24 的终端访问 Web Server1 的访问控制策略。

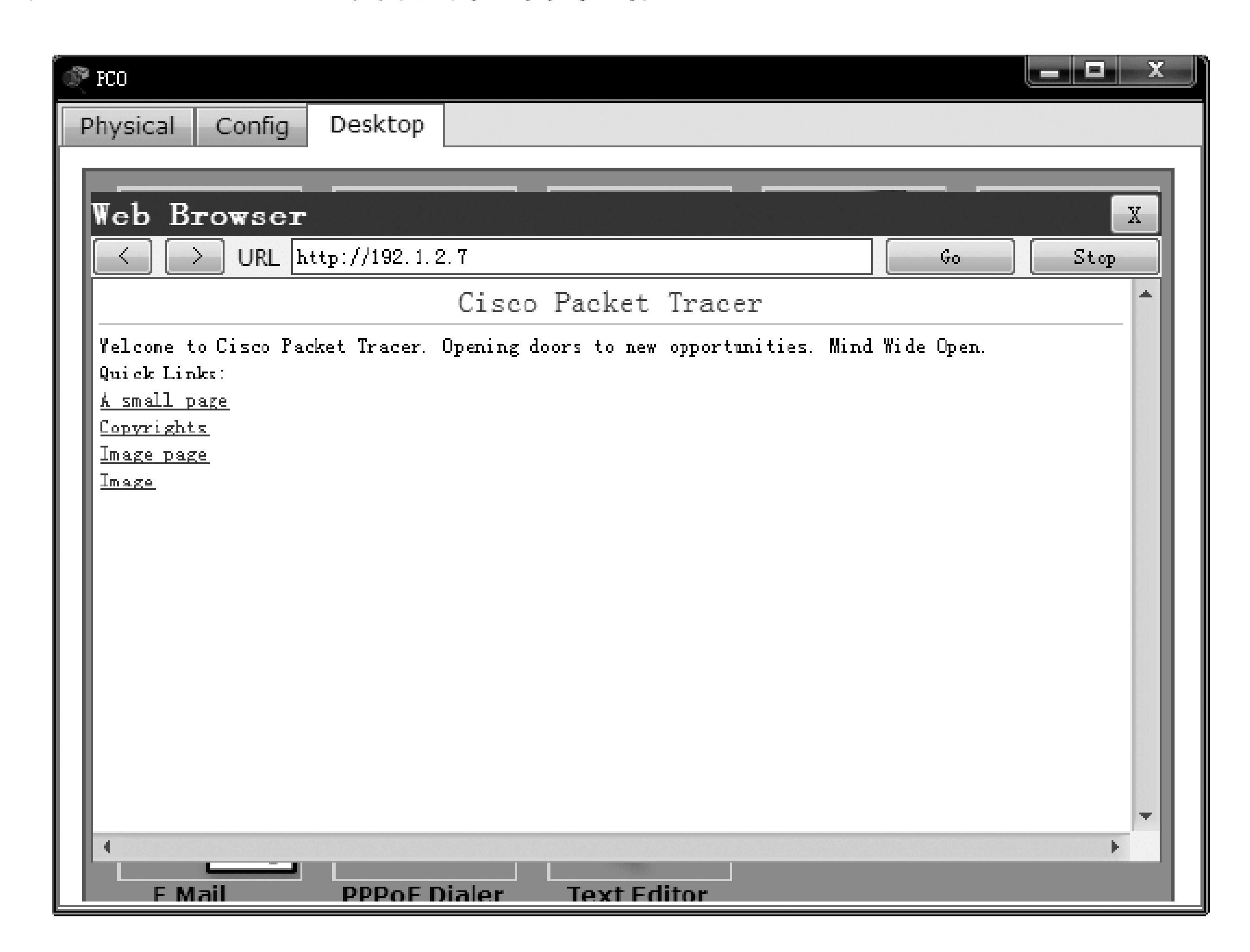


图 9.14　PC0 成功访问 Web Server1 界面

(5) PC0 通过在 E-mail Server1 上注册的用户向在 E-mail Server2 上注册的用户发送邮件,同时接收在 E-mail Server2 上注册的用户发送的邮件。PC1 通过在 E-mail Server2 上注册的用户向在 E-mail Server1 上注册的用户发送邮件,同时接收在 E-mail Server1 上注册的用户发送的邮件,以此验证允许属于网络 192.1.1.0/24 的终端通过 SMTP 和 POP3 访问 E-mail Server1,允许 E-mail Server1 和 E-mail Server2 通过 SMTP 实现互访的访问控制策略。图 9.15 是在 E-mail Server1 上注册用户的界面。图 9.16 是在 E-mail Server2 上注册用

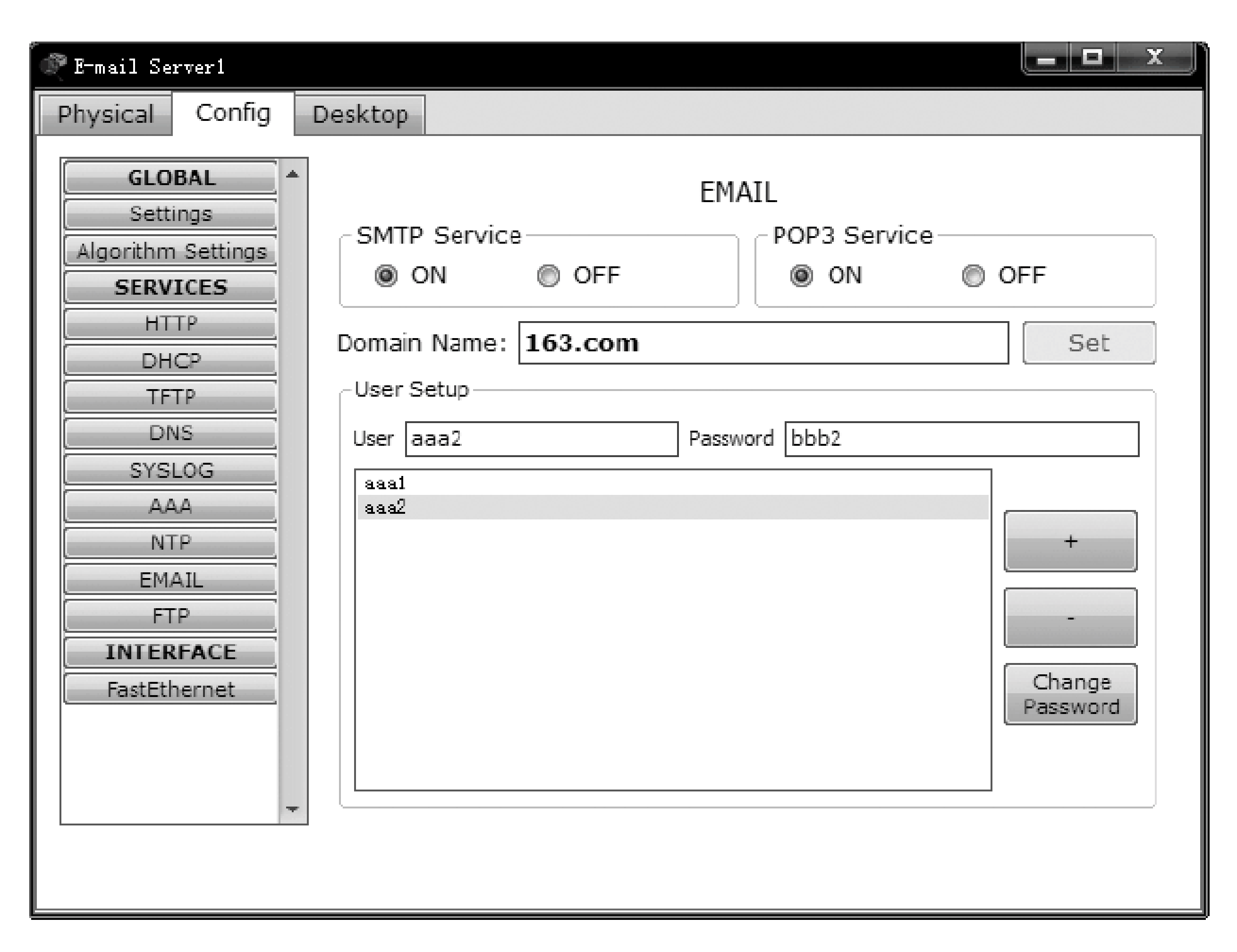


图 9.15　E-mail Server1 注册用户界面

户的界面。为了能够用域名 163.com 和域名 263.com 访问 E-mail Server1 和 E-mail Server2,需要在各个网络中配置域名服务器,网络 192.1.1.0/24 用 FTP Server 作为域名服务器,网络 192.1.2.0/24 用 Web Server1 作为域名服务器,网络 192.1.3.0/24 用 Web Server2 作为域名服务器,因此,网络 192.1.1.0/24 中的终端需配置域名服务器 IP 地址 192.1.1.7。E-mail Server1 需配置域名服务器 IP 地址 192.1.2.7。网络 192.1.3.0/24 中的终端和 E-mail Server2 需配置域名服务器 IP 地址 192.1.3.7。图 9.17 是 Web Server2 配置资源记录的界面。图 9.18 是 PC0 配置信箱的界面。图 9.19 是 PC0 编辑和发送邮件的界面,PC0 向信箱 ccc1@263.com 发送一封邮件。图 9.20 是 PC1 配置信箱界面。图 9.21 是 PC1 接收来自信箱 aaa1@163.com 的邮件的界面。同样,PC0 可以接收来自信箱 ccc1@263.com 的邮件。

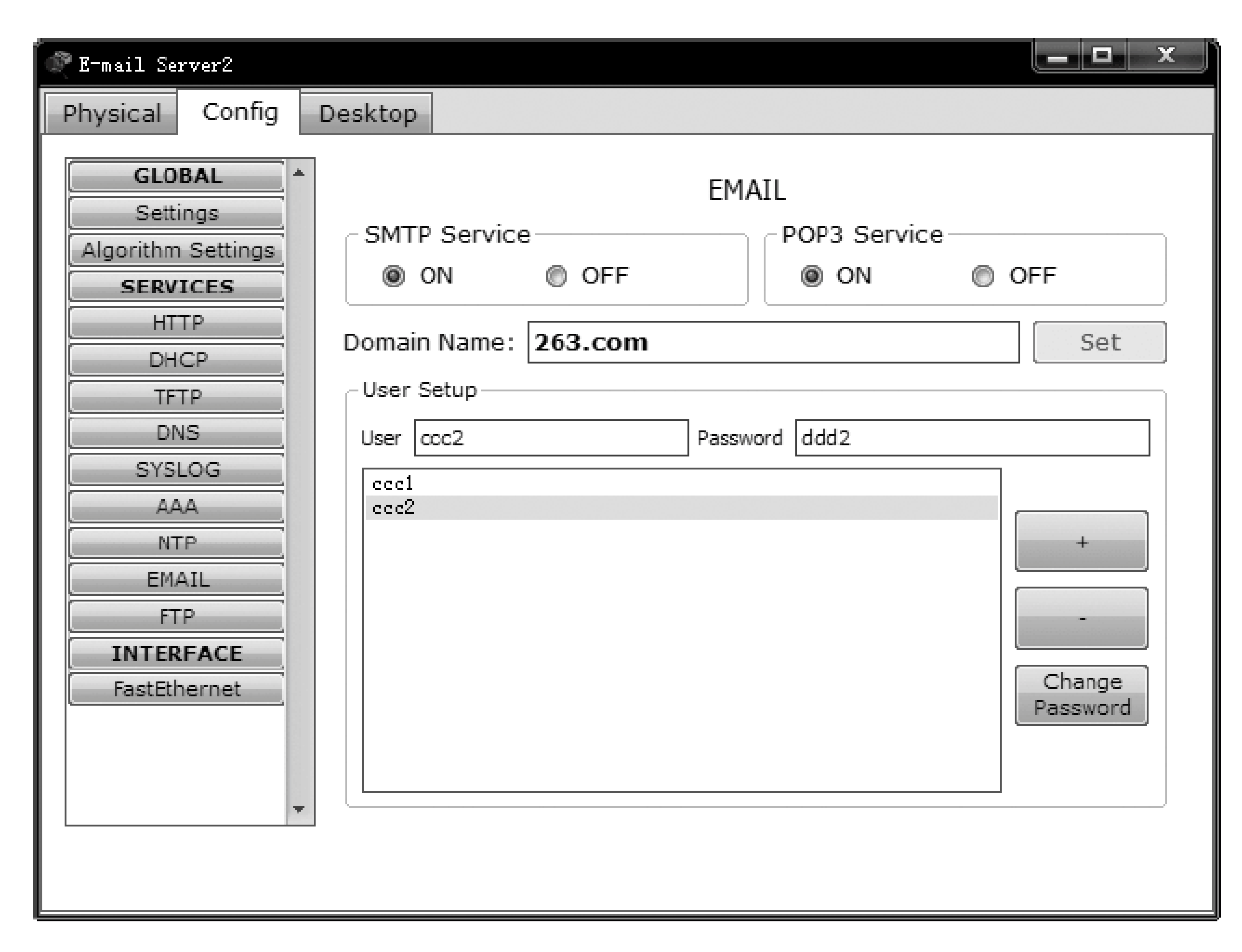


图 9.16 E-mail Server2 注册用户界面

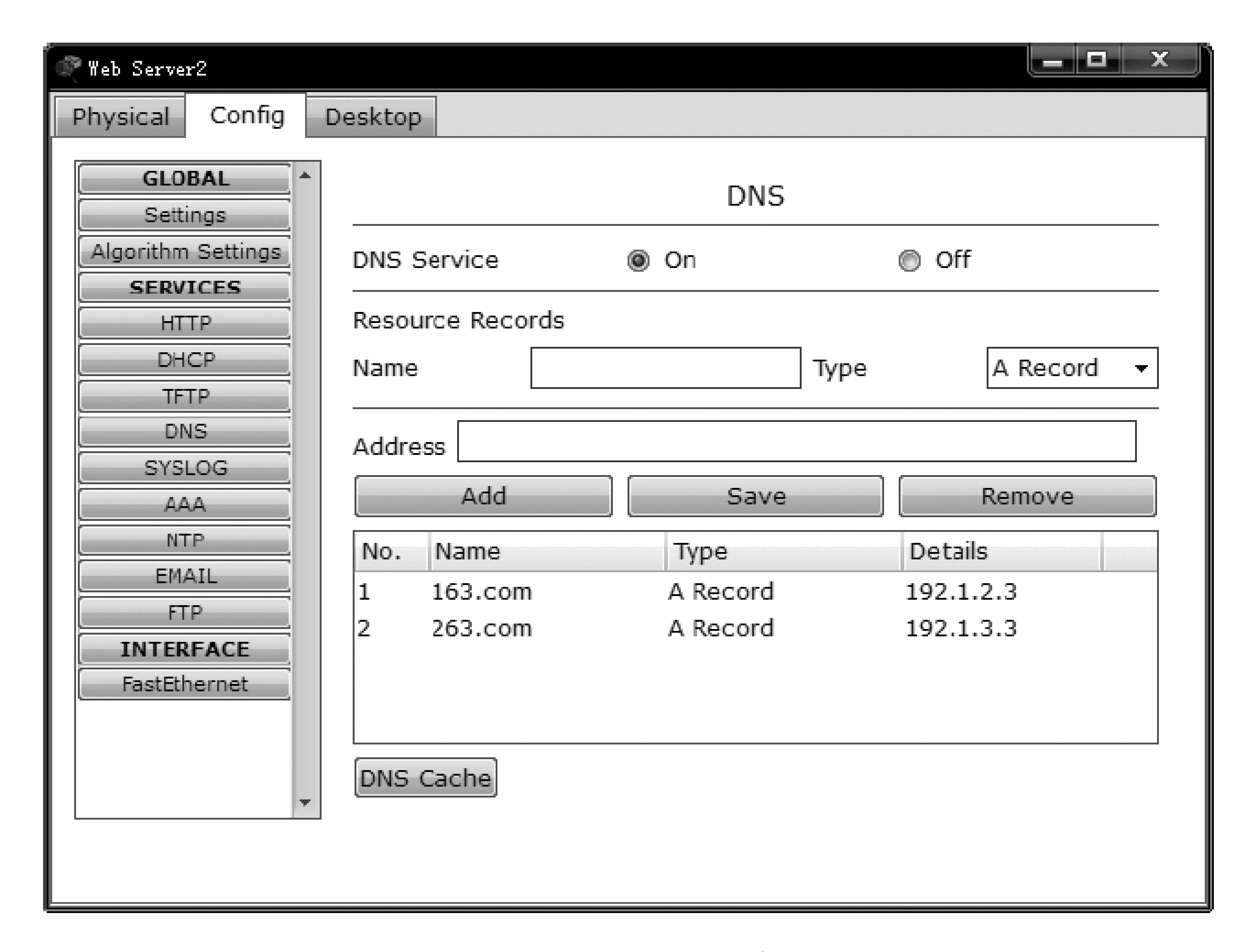


图 9.17 Web Server2 配置资源记录界面

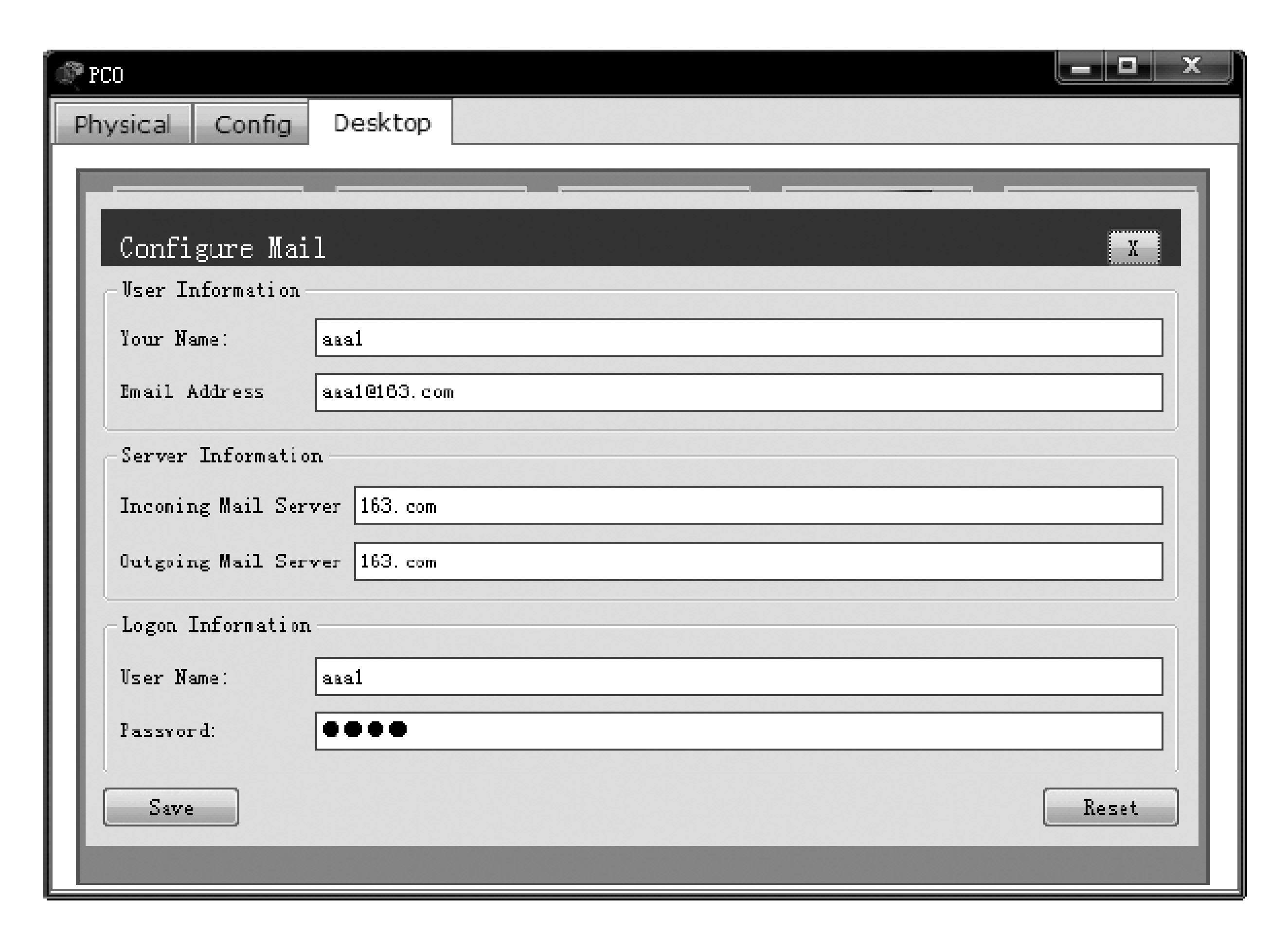


图 9.18　PC0 配置信箱界面



图 9.19　PC0 编辑和发送邮件界面



图 9.20　PC1 配置信箱界面

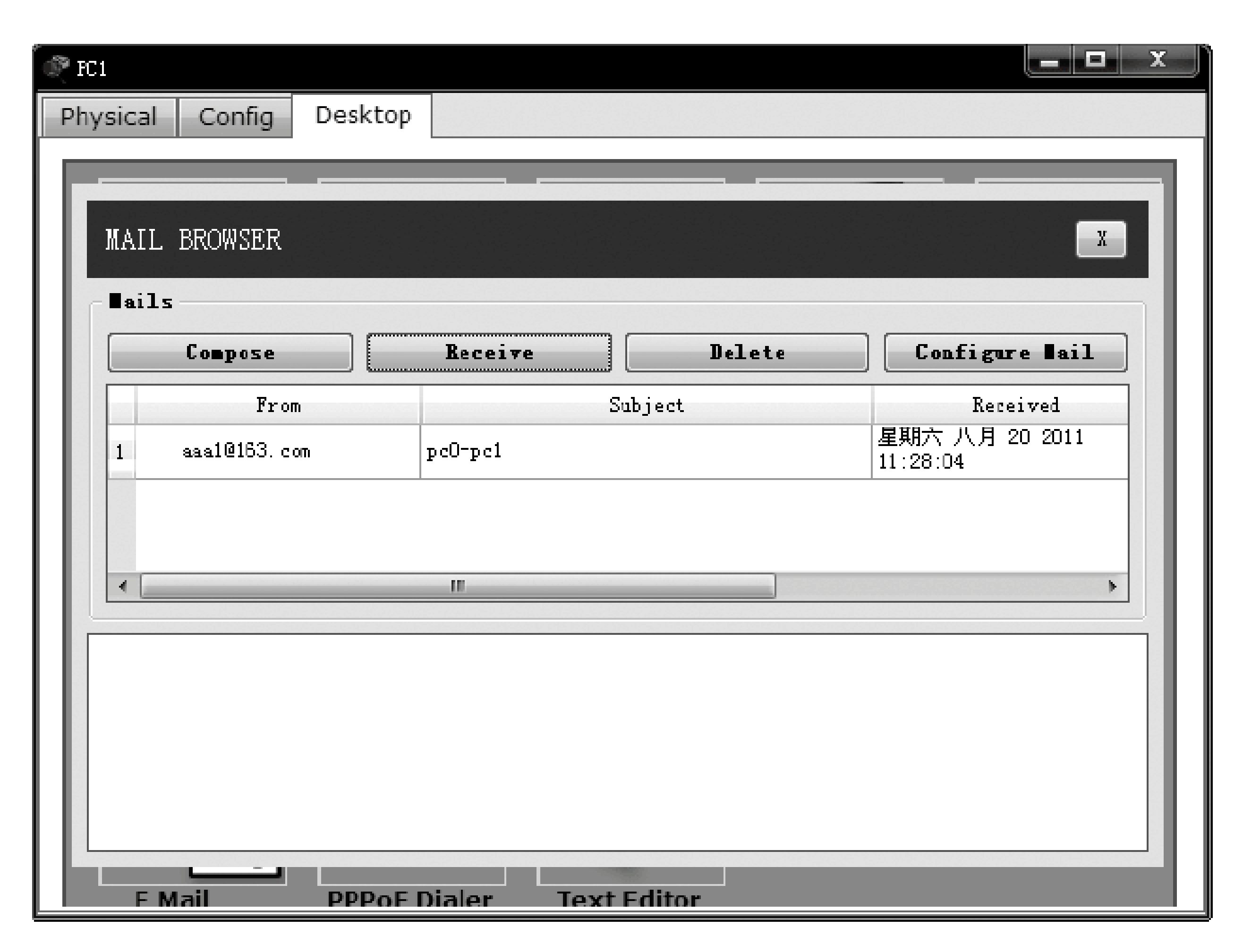


图 9.21 PC1 接收邮件界面

(6) 可以通过 PC1 访问 FTP Server 失败、PC0 无法连接信箱 ccc1@263.com、PC1 无法连接信箱 aaa1@163.com，证明无法进行访问控制策略不允许的访问过程。

4. 命令行配置过程

(1) Router1 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.1 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.1.0
Router(config-router)#network 192.1.4.0
Router(config-router)#exit
```

(2) Router2 基本命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.4.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
```

```
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.5.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.4.0
Router(config-router)#network 192.1.5.0
Router(config-router)#exit
```

（3）Router3 命令行配置过程。

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.5.2 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.3.254 255.255.255.0
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.3.0
Router(config-router)#network 192.1.5.0
Router(config-router)#exit
```

（4）Router2 有状态分组过滤器命令行配置过程。

```
Router(config)#access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www
Router(config)#access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
Router(config)#access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq pop3
Router(config)#access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7 eq www
Router(config)#access-list 111 permit udp host 192.1.4.1 eq 520 any eq 520
                    (允许 Router1 发送的 RIP 路由消息进入 Router2,封装 RIP 路由消息的 UDP 报文的
                     源和目的端口号均为 520)
Router(config)#access-list 112 permit udp host 192.1.4.2 eq 520 any eq 520
                    (允许 Router2 向 Router1 发送 RIP 路由消息)
Router(config)#ip inspect name a11 http
Router(config)#ip inspect name a11 tcp
                    (通过检测传输层协议 TCP 代替检测应用层协议 SMTP 和 POP3)
Router(config)#access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7 eq www
Router(config)#access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq smtp
```

```
Router(config)#access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3 eq pop3
Router(config)#access-list 121 permit tcp host 192.1.3.3 host 192.1.2.3 eq smtp
Router(config)#access-list 121 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7 eq www
Router(config)#access-list 122 permit tcp host 192.1.2.3 host 192.1.3.3 eq smtp
Router(config)#ip inspect name a121 http
Router(config)#ip inspect name a121 tcp
Router(config)#ip inspect name a122 tcp
Router(config)#access-list 131 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7 eq www
Router(config)#access-list 131 permit tcp host 192.1.2.3 host 192.1.3.3 eq smtp
Router(config)#access-list 131 permit udp host 192.1.5.1 eq 520 any eq 520
                                        (允许 Router2 向 Router3 发送 RIP 路由消息)
Router(config)#access-list 132 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7 eq www
Router(config)#access-list 132 permit tcp host 192.1.3.3 host 192.1.2.3 eq smtp
Router(config)#access-list 132 permit udp host 192.1.5.2 eq 520 any eq 520
                                        (允许 Router3 发送的 RIP 路由消息进入 Router2)
Router(config)#ip inspect name a131 http
Router(config)#ip inspect name a131 tcp
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 111 in
Router(config-if)#ip access-group 112 out
Router(config-if)#ip inspect a111 in
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 131 out
Router(config-if)#ip access-group 132 in
Router(config-if)#ip inspect a131 in
Router(config-if)#ip inspect a131 out
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip access-group 121 out
Router(config-if)#ip access-group 122 in
Router(config-if)#ip inspect a121 out
Router(config-if)#ip inspect a122 in
Router(config-if)#exit
```

9.3.4 区域策略防火墙配置实验

1. 实验内容

(1) 完成区域划分。

(2) 分类区域间传输的信息流。

(3) 配置区域间访问控制策略。

(4) 验证区域策略防火墙控制区域间数据交换的过程。

2. 网络结构

网络结构如图 9.9 所示。将路由器 R2 接口 1 连接的网络定义为信任区,接口 2 连接的

网络定义为非军事区，接口 3 连接的网络定义为非信任区。同时将接口 1 分配给信任区，接口 2 分配给非军事区，接口 3 分配给非信任区，要求实现以下区域间访问控制策略。

① 信任区至非军事区，地址属于 192.1.1.0/24 中的终端通过 HTTP 访问地址为 192.1.2.7/32 的 Web 服务器 1。

② 信任区至非军事区，地址属于 192.1.1.0/24 中的终端通过 SMTP 和 POP3 访问地址为 192.1.2.3/32 的 E-mail 服务器 1。

③ 信任区至非信任区，地址属于 192.1.1.0/24 中的终端通过 HTTP 访问地址为 192.1.3.7/32 的 Web 服务器 2。

④ 非军事区至非信任区，地址为 192.1.2.3/32 的 E-mail 服务器 1 通过 SMTP 访问地址为 192.1.3.3/32 的 E-mail 服务器 2。

⑤ 非信任区至非军事区，地址属于 192.1.3.0/24 中的终端通过 HTTP 访问地址为 192.1.2.7/32 的 Web 服务器 1。

⑥ 非信任区至非军事区，地址为 192.1.3.3/32 的 E-mail 服务器 2 通过 SMTP 访问地址为 192.1.2.3/32 的 E-mail 服务器 1。

⑦ 禁止其他一切区域间数据交换过程。

3. 实验步骤

路由器 Router1、Router3、终端和服务器的配置过程及 Router2 的基本配置过程与 9.3.3 节有状态分组过滤器配置实验完全相同，不同的是 Router2 的区域防火墙配置。Router2 区域防火墙配置过程参见 9.1.3 节中的配置过程部分。

4. Router2 区域防火墙命令行配置过程

```
Router(config)#access-list 111 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.7
Router(config)#access-list 112 permit tcp 192.1.1.0 0.0.0.255 host 192.1.2.3
Router(config)#class-map type inspect match-all trust-dmz-http
Router(config-cmap)#match access-group 111
*Router(config-cmap)#match protocol http
Router(config-cmap)#exit
Router(config)#class-map type inspect match-all trust-dmz-smtp
Router(config-cmap)#match access-group 112
Router(config-cmap)#match protocol smtp
Router(config-cmap)#exit
Router(config)#class-map type inspect match-all trust-dmz-pop3
Router(config-cmap)#match access-group 112
Router(config-cmap)#match protocol pop3
Router(config-cmap)#exit
Router(config)#policy-map type inspect trust-dmz
Router(config-pmap)#class type inspect trust-dmz-http
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#class type inspect trust-dmz-smtp
Router(config-pmap-c)#inspect
```

```
Router(config-pmap-c)#exit
Router(config-pmap)#class type inspect trust-dmz-pop3
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#access-list 121 permit tcp 192.1.1.0 0.0.0.255 host 192.1.3.7
Router(config)#class-map type inspect match-all trust-notrust
Router(config-cmap)#match access-group 121
*Router(config-cmap)#match protocol http
Router(config-cmap)#exit
Router(config)#policy-map type inspect trust-notrust
Router(config-pmap)#class type inspect trust-notrust
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#access-list 131 permit tcp host 192.1.2.3 host 192.1.3.3
Router(config)#class-map type inspect match-all dmz-notrust
Router(config-cmap)#match access-group 131
Router(config-cmap)#match protocol smtp
Router(config-cmap)#exit
Router(config)#policy-map type inspect dmz-notrust
Router(config-pmap)#class type inspect dmz-notrust
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#access-list 141 permit tcp 192.1.3.0 0.0.0.255 host 192.1.2.7
Router(config)#access-list 142 permit tcp host 192.1.3.3 host 192.1.2.3
Router(config)#class-map type inspect match-all notrust-dmz-http
Router(config-cmap)#match access-group 141
*Router(config-cmap)#match protocol http
Router(config-cmap)#exit
Router(config)#class-map type inspect match-all notrust-dmz-smtp
Router(config-cmap)#match access-group 142
Router(config-cmap)#match protocol smtp
Router(config-cmap)#exit
Router(config)#policy-map type inspect notrust-dmz
Router(config-pmap)#class type inspect notrust-dmz-http
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#class type inspect notrust-dmz-smtp
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#zone security trust
```

```
Router(config-sec-zone)#exit
Router(config)#zone security notrust
Router(config-sec-zone)#exit
Router(config)#zone security dmz
Router(config-sec-zone)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#zone-member security trust
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#zone-member security notrust
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#zone-member security dmz
Router(config-if)#exit
Router(config)#zone-pair security trust-dmz source trust destination dmz
Router(config-sec-zone-pair)#service-policy type inspect trust-dmz
Router(config-sec-zone-pair)#exit
Router(config)#zone-pair security trust-notrust source trust destination notrust
Router(config-sec-zone-pair)#service-policy type inspect trust-notrust
Router(config-sec-zone-pair)#exit
Router(config)#zone-pair security dmz-notrust source dmz destination notrust
Router(config-sec-zone-pair)#service-policy type inspect dmz-notrust
Router(config-sec-zone-pair)#exit
Router(config)#zone-pair security notrust-dmz source notrust destination dmz
Router(config-sec-zone-pair)#service-policy type inspect notrust-dmz
Router(config-sec-zone-pair)#exit
Router(config)#
```

注意：带 * 号的命令在 Packet Tracer 5.3 中使用时存在问题，实际配置时不需输入。

第10章 入侵防御系统

CHAPTER

10.1 知识要点

10.1.1 入侵防御系统定义和分类

1. 入侵防御系统定义

入侵是一系列试图破坏信息资源完整性、保密性和可用性的行为。

入侵检测是一种用于检测出任何破坏或试图破坏信息资源完整性、保密性和可用性的行为的机制。

入侵防御系统是一种通过从计算机网络系统中的若干关键结点收集信息、分析信息，以此检测出网络中违反安全策略或入侵的行为，并对这些行为予以反制的网络安全技术。

2. 入侵防御系统分类

入侵防御系统根据收集信息的地点和实施保护的对象不同可以分为主机入侵防御系统(Host Intrusion Prevention System，HIPS)和网络入侵防御系统(Network Intrusion Prevention System，NIPS)。主机入侵防御系统主要对到达某台主机的信息流进行检测，对主机资源的访问操作实施监控，以此保护主机资源免遭攻击。网络入侵防御系统主要对流经网络某段链路的信息流进行检测，对发生在网络中的行为实施监控，发现攻击行为并对攻击行为实施反制。

3. 入侵检测系统和入侵防御系统的区别

入侵检测系统只是嗅探信息，如图10.1(a)所示。将连接集线器的网卡设置成混杂(Promiscuous)模式，允许接收任意目的MAC地址的MAC帧，但无法对MAC帧传输过程发生影响，因此只能检测到入侵行为，并通过报警等方式发出警告，但无法对与入侵行为有关的MAC帧传输过程实施干预。

经过关键链路传输的信息流需要经过入侵防御系统，如图10.1(b)所示。入侵防御系统一旦检测到与攻击行为相关的信息流，可以立即实施干预，如丢弃与攻击行为相关的IP分组，通过动态增加过滤规则，禁止和这些IP分

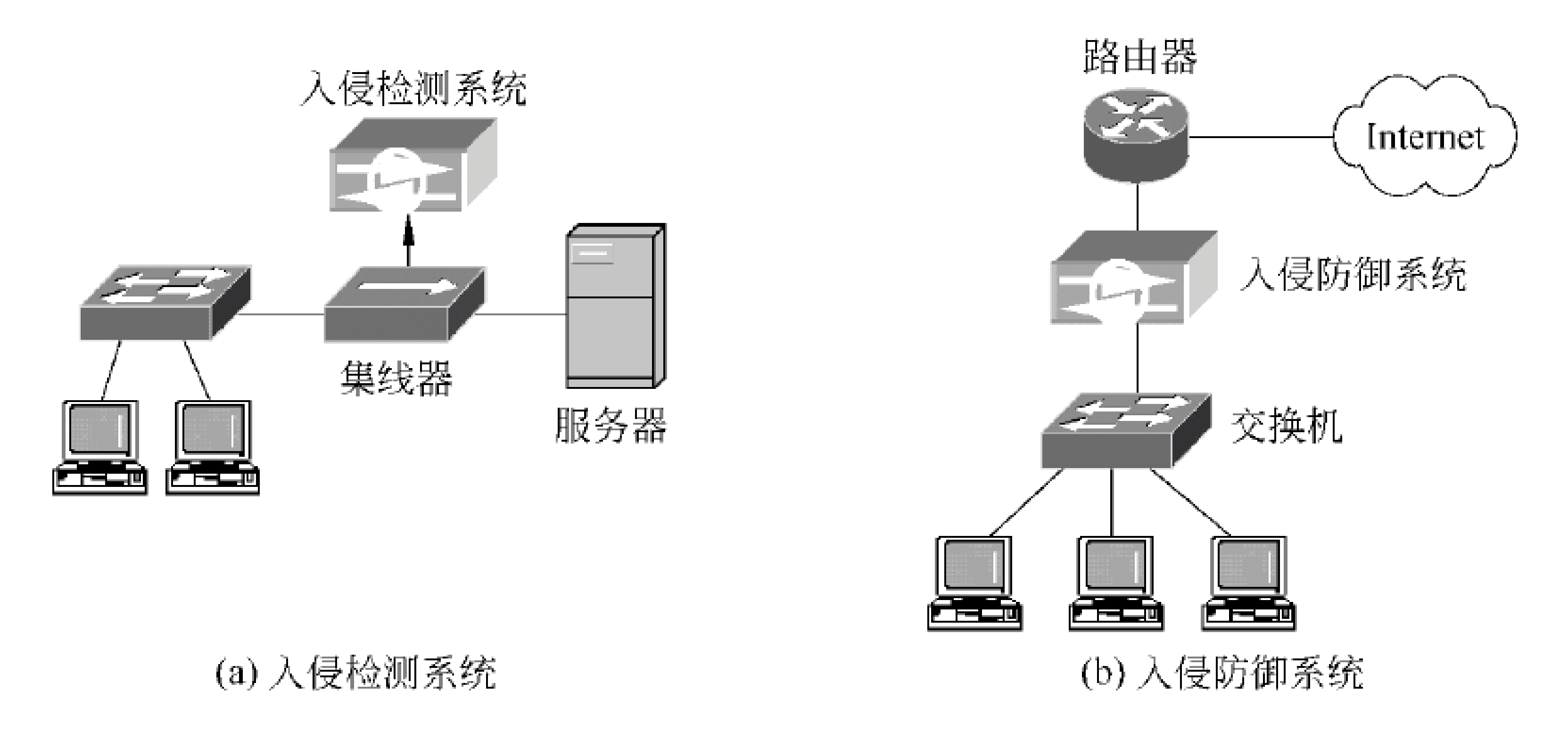


图 10.1 入侵检测系统和入侵防御系统的区别

组有着相同源 IP 地址的 IP 分组正常转发等。

入侵检测系统和入侵防御系统的区别在于前者只是被动收集、分析信息，在检测到攻击行为后，通过报警等方式向网络安全管理员示警，但无法实时实施反制动作。后者由于承担信息流转发功能，一旦发现攻击行为，可以实时实施反制动作。

10.1.2 入侵检测机制

1. 攻击特征检测

攻击特征检测，也称为滥用检测，和杀毒软件检测病毒的机制相同，从已经发现的攻击中提取出能够标识这一攻击的特征信息，构成攻击特征库，然后在捕获到的信息中进行攻击特征匹配操作，如果匹配到某个攻击特征，说明捕获到的信息就是攻击信息。

2. 协议译码

协议译码一是对 IP 分组格式、TCP 报文格式进行检测，二是根据 TCP 报文的目的端口字段值或 IP 报文的协议字段值确定报文净荷对应的应用层协议，然后根据协议要求对净荷格式、净荷中各字段内容及请求和响应过程进行检测，如果发现和协议要求不一致的地方，表明该信息可能是攻击信息。

3. 异常检测

异常检测首先建立正常网络访问过程下的信息流模式或正常网络访问规则，然后实时分析捕获到的信息所反映的信息流模式或对网络资源的操作，并将分析结果和已经建立的信息流模式库或操作规则库相比较，如果发现较大偏差，说明发现异常信息。

10.1.3 反制动作

1. 丢弃 IP 分组

丢弃 IP 分组首先丢弃单个包含元攻击特征的 IP 分组，然后通过动态增加过滤规则，或者禁止和该 IP 分组源 IP 地址相同的 IP 分组，或者禁止和该 IP 分组目的 IP 地址相同的 IP 分组，或者禁止和该 IP 分组源和目的 IP 地址相同的 IP 分组正常转发。通常需要为动态过滤规则设置时间阈值，一旦时间阈值到，自动删除该过滤规则，恢复正常数据传输过程。

2. 释放 TCP 连接

一旦检测到异常信息,而该异常信息又属于某个 TCP 连接,入侵防御系统通过向该 TCP 连接的发起端或响应端发送 RST 位置 1 的 TCP 控制报文来释放该 TCP 连接。由于图 10.1(a)所示的系统也可实施这种反制动作,因此目前也存在采用图 10.1(a)所示的信息收集方式的入侵防御系统。

10.1.4 元攻击特征实例

表 10.1 所示是一些元攻击特征实例。

表 10.1 元攻击特征实例

IP 分组/TCP 报文特征	可能存在的攻击
IP 首部携带严格的源站选路	网络探测
源 IP 地址和目的 IP 地址相同	Land 攻击
源 IP 地址为 127.0.0.1	源 IP 地址欺骗攻击
源 IP 地址为 255.255.255.255	源 IP 地址欺骗攻击
IP 首部协议字段=1、标志位 MF=1、片偏移×8+长度>64KB	Ping Of Death 攻击
发送给特定主机,SYN=0、ACK=0、RST=0、FIN=0 的 TCP 报文	目标侦察
发送给特定主机,SYN=1、FIN=1 的 TCP 报文	目标侦察
源端口号= 12345,SYN=1、ACK=1 的 TCP 报文	木马
源端口号= 31337,SYN=1、ACK=1 的 TCP 报文	木马

10.2 例题解析

10.2.1 自测题

1. 选择题

(1) 对于入侵防御系统,下述________的描述是错误的。

A. 一般的入侵防御系统和杀毒软件一样,需要定时更新攻击特征库

B. 正常访问过程和入侵过程存在差异,但无法严格区分

C. 规则是长期观察信息流变化过程后得出的一些规律性的总结

D. 入侵防御系统能够检测出没有发作的病毒

(2) 下述________是入侵防御系统和入侵检测系统的区别。

A. 需要定时更新攻击特征库　　　　B. 收集流经某段链路的信息

C. 检测信息中是否包含攻击特征　　D. 丢弃包含攻击特征的信息

(3) 对于入侵检测机制,下述________描述是错误的。

A. 检测某些字段取值是否超出正常范围
B. 检测流量分布是否和正常访问过程相似
C. 检测信息中是否包含攻击特征
D. 检测信息传输过程中是否被篡改

(4) 下述________是入侵防御系统和防火墙相同的功能。
A. 利用攻击特征库发现攻击行为　B. 作用于流经任何网段的信息
C. 阻断正常信息传输　D. 阻断非法信息传输

(5) 对于主机入侵防御系统，下述________描述是错误的。
A. 利用攻击特征库发现攻击行为　B. 根据访问授权发现非法资源访问
C. 禁止非法 TCP 连接建立　D. 保证主机不感染病毒

(6) 下述________不是产生入侵防御系统的原因。
A. 与攻击有关的信息流无处不在
B. 攻击行为与正常访问过程存在差别
C. 杀毒软件不具有发现非法资源访问操作的功能
D. 控制网络间数据交换过程

(7) 下述________描述是错误的。
A. 单个 IP 分组可以包含全部元攻击特征
B. 元攻击特征可能分散在因为分片产生的多个 IP 分组中
C. 有状态攻击特征(组合攻击特征)需要记录状态迁移路径
D. 有状态攻击特征只能分布在属于同一 TCP 连接的多个 TCP 报文中

(8) 下述________描述是错误的。
A. 攻击特征检测机制容易漏报
B. 异常检测机制容易误报
C. 协议译码能够检测出恶意错误
D. 攻击特征检测机制能够检测出未知攻击

(9) 下述________关于入侵防御系统功能的描述是错误的。
A. 防御病毒发作引发的攻击行为　B. 防御对资源的非法访问
C. 防御分布式拒绝服务攻击　D. 防御信息嗅探和截获攻击

(10) 下述________是入侵防御系统能够防御的攻击行为。
A. 路由项欺骗攻击　B. 重放攻击
C. DNS 欺骗攻击　D. 源 IP 地址欺骗攻击

2. 填空题

(1) 入侵防御系统分为________和________。

(2) 入侵防御系统工作过程分为________、________、________和________。

(3) 入侵检测机制有________、________和________，其中________只能检测已知攻击行为，________容易误报。

(4) 入侵防御系统最大的问题是容易发生________和________，其中________误把正常访问过程当作攻击，________误把攻击当作正常访问过程。

(5) 入侵检测系统用于检测异常信息流,定义为异常的信息流有________、________和________,因此,配置入侵检测系统需要配置________、________和________。

3. 名词解释

____攻击特征检测　　____协议译码
____漏报　　____入侵检测系统
____入侵　　____入侵检测机制
____异常检测　　____元特征
____主机入侵防御系统　　____网络入侵防御系统
____有状态特征(组合特征)　　____误报

(a) 一系列试图破坏信息资源完整性、保密性和可用性的行为。

(b) 一种用于检测出任何破坏或试图破坏信息资源完整性、保密性和可用性的行为的机制。

(c) 一种通过对到达主机的信息进行检测,对主机资源访问过程实施监控,以此检测出对主机的入侵,和对主机资源的非法访问操作,并对这些行为予以反制的网络安全技术。

(d) 一种通过从网络中的关键结点,或关键链路收集信息、分析信息,以此检测出网络中违反安全策略或入侵的行为,并对这些行为予以反制的网络安全技术。

(e) 一种通过分析已经发现的攻击,提取出能够标识这些攻击的特征信息,构成攻击特征库,然后在捕获到的信息中进行攻击特征匹配操作,以此发现攻击行为的入侵检测机制。

(f) 一种通过检测各层 PDU 中控制信息的字段值和正常取值范围之间是否存在较大偏差来发现攻击行为的入侵检测机制。

(g) 一种首先建立用于描述正常访问过程的行为模式(正常行为模式),然后通过判断检测到的用户行为与正常行为模式之间是否存在较大偏差来确定该用户行为是否是攻击行为的入侵检测机制。

(h) 描述单一事件的特征(如包含特定字符串,源 IP 地址与目的 IP 地址相同的 IP 分组),一旦检测到该单一事件,就可确定发生攻击行为。

(i) 描述一系列分布在某个访问过程中事件的特征,只有在指定访问过程中检测到这些事件顺序发生,才能确定发生攻击行为。

(j) 将正常行为当作攻击行为,并发出警报的事件。

(k) 未能检测出攻击行为的事件。

(l) 一种以嗅探方式收集信息,分析信息,以此检测出网络中违反安全策略或入侵的行为,并通过报警或事后弥补方式对攻击行为进行干预的网络安全技术。由于是以嗅探方式收集信息,因此无法阻止恶意信息继续传输。

4. 判断题

(1) 入侵防御系统可以代替防火墙。

(2) 入侵防御系统只能检测网络内部传输的信息流。

(3) 入侵检测系统的干预行为往往滞后攻击行为。

(4) 入侵防御系统能够实时反制攻击行为。
(5) 攻击特征检测容易漏报。
(6) 异常检测容易误报。
(7) 异常检测能够检测出未知攻击。
(8) 主机入侵防御系统能够阻止对主机信息资源的非法访问。
(9) 分析主机日志是一项保证主机安全的重要工作。
(10) 入侵防御系统能够有效阻止病毒传播。
(11) 入侵防御系统能够有效阻止已知木马外泄主机信息资源。
(12) 入侵防御系统能够有效防御黑客攻击。
(13) 入侵防御系统能够有效弥补操作系统和应用程序漏洞。
(14) 使用异常检测机制的产品不多。
(15) 入侵防御系统在阻止病毒传播和防御黑客攻击方面优于防火墙。
(16) 入侵防御系统更多地与交换机和路由器集成在一起。

10.2.2 自测题答案

1. 选择题答案

(1) D,入侵防御系统主要检测发生在主机和网络中的异常行为,病毒不发作时,并不发生异常行为。

(2) D,这是以嗅探方式收集信息的入侵检测系统无法做到的。

(3) D,这是目的终端的完整性检测功能,不属于入侵检测机制的检测范围。

(4) D,防火墙阻断访问控制策略不允许传输的信息,入侵防御系统阻断违反安全策略,或实施攻击的信息。

(5) D,检测某个文件是否包含病毒不是入侵防御系统的主要功能,入侵防御系统主要检测病毒发作时发生的异常行为。

(6) D,这是防火墙已经实现的功能。

(7) D,访问过程不一定基于 TCP,如域名解析过程。

(8) D,通过分析已经发现的攻击行为,才能提取该攻击行为的特征信息。

(9) D,这是需要通过增强网络设备的安全功能才能防御的攻击。

(10) D,有些源 IP 地址欺骗攻击采用固定格式的源 IP 地址,攻击特征检测机制能够检测此类源 IP 地址欺骗攻击。

2. 填空题答案

(1) 主机入侵防御系统,网络入侵防御系统。

(2) 收集信息,检测入侵行为,反制入侵行为,登记和分析。

(3) 攻击特征检测,协议译码,异常检测,攻击特征检测,异常检测。

(4) 误报,漏报,误报,漏报。

(5) 和某个攻击特征匹配的信息流,包含违背协议规定内容的信息流,超过设定阈值或违背统计规律的信息流,攻击特征库,限制信息交换过程的协议列表和发送端、接收端地址范围,统计阈值和规则。

3. 名词解释答案

e 攻击特征检测	f 协议译码
k 漏报	l 入侵检测系统
a 入侵	b 入侵检测机制
g 异常检测	h 元特征
c 主机入侵防御系统	d 网络入侵防御系统
i 有状态特征(组合特征)	j 误报

4. 判断题答案

(1) 错,入侵防御系统并不具备根据访问控制策略控制网络间数据交换过程的功能。

(2) 错,入侵防御系统可以检测流经任何网段,或经过任何网络结点的信息流,包括路由器转发的信息流。

(3) 对,入侵检测系统一般无法阻断攻击信息继续传输。

(4) 对,入侵防御系统能够丢弃实施攻击的信息。

(5) 对,无法检测出未知攻击。

(6) 对,攻击行为和正常访问过程不存在严格区别。

(7) 对,攻击行为一旦偏离描述正常访问过程的行为模式,就会被异常检测机制发现。

(8) 对,可以配置主机资源访问控制列表,实现授权访问。

(9) 对,日志记录了用户对主机的全部操作,通过分析日志可以发现非法操作。

(10) 对,病毒传播往往引发异常行为,可以被入侵防御系统发现。

(11) 对,木马往往有固定的 TCP 连接端口,可以通过在攻击特征库中加入元特征——固定源端口号的 TCP 连接响应来阻断木马建立 TCP 连接。

(12) 对,黑客攻击有固定的行为模式,可以通过在攻击特征库中加入描述黑客攻击行为的有状态特征来阻断黑客和被攻击主机之间的传输通路。

(13) 对,黑客利用已知的漏洞实施的攻击有固定的行为模式,可以通过在攻击特征库中加入描述黑客攻击行为的有状态特征来阻断黑客和存在漏洞的主机之间的传输通路。

(14) 对,异常检测需要建立描述正常访问过程的行为模式,这与网络的应用环境有关,与使用网络的时段有关,必须动态调整,除非是自学习系统,否则很少有用户具备完成这一工作的能力。

(15) 对,通过不断更新攻击特征库,可以使入侵防御系统阻断大量已知病毒传播过程,防御大量已知黑客攻击行为。

(16) 对,网络转发结点容易收集信息,容易丢弃攻击信息。

10.2.3　简答题解析

1. 简述产生入侵防御系统的原因。

回答:产生入侵防御系统的原因在于:一是碰到现有技术无法解决的问题,二是找到解决这些问题的新的方法。具体在于:一是攻击信息无处不在,仅仅通过防火墙对网

络间数据交换过程实施控制已无法阻止攻击信息扩散;二是攻击行为与正常访问过程之间存在差异,这种差异可以通过建立攻击特征库和描述正常访问过程的行为模式检测出来;三是可以通过建立资源访问控制列表,实施主机资源的授权访问,同时也可以通过资源访问控制列表检测出非法资源访问操作;四是交换机、路由器等网络设备既容易实现信息收集,又容易阻断攻击信息传输。上述原因导致产生或是与交换机、路由器集成在一起,或是运行于主机系统,通过在网络关键结点,或关键链路收集信息,分析信息,检测出非法访问操作、违反安全策略和入侵的行为,并对这些行为予以反制的设备。

2. 简述网络入侵防御系统和防火墙的区别。

回答:一是检测的信息不同,防火墙只检测网络间传输的信息,入侵防御系统能够检测流经任何网段的信息。二是检测机制不同,防火墙根据配置的访问控制策略确定信息是否违反安全策略,并丢弃违反安全策略的信息,入侵防御系统根据建立的攻击特征库和描述正常访问过程的行为模式确定是否是攻击信息,并对攻击信息予以反制。三是作用不同,防火墙的作用是通过静态配置访问控制策略来限制网络间允许交换的信息流类型,入侵防御系统通过分析已经发现的入侵行为,如蠕虫传播过程、木马窃取信息资源过程和黑客利用操作系统漏洞实施的攻击过程,提取出攻击特征,通过对这些攻击特征的匹配操作,可以检测出正在进行的攻击行为,并予以反制,因此入侵防御系统的主要作用是阻止已知的和未知的攻击行为继续。四是入侵防御系统通过在多个关键结点和关键链路收集信息,并对这些信息的检测结果进行综合分析来发现分布式拒绝服务攻击,和其他对网络的侦察行为,防火墙不具有这一功能。

3. 简述主机入侵防御系统和网络入侵防御系统的区别。

回答:一是收集的信息不同,主机入侵防御系统只收集进出主机的信息,网络入侵防御系统收集流经任何网段的信息。二是作用不同,主机入侵防御系统主要用于阻止对主机资源的非法操作,网络入侵防御系统是阻止已知和未知的攻击行为继续,这些攻击行为包括蠕虫传播过程、木马窃取信息资源过程和黑客利用操作系统漏洞实施的攻击过程等。三是保护对象不同,网络入侵防御系统保护网段后面的多个主机、多段网段,甚至一个网络,主机入侵防御系统只保护单个主机系统。四是主机入侵防御系统能够截获有关用户、进程、访问对象和访问方式等信息,可以利用这些信息实施精确监控,网络入侵防御系统收集的有关资源访问操作的信息不及主机入侵防御系统详细。五是主机入侵防御系统可以通过配置资源访问控制列表实施授权访问,网络入侵防御系统不具有这一功能。

4. 简述网络入侵防御系统的实现机制。

回答:一是收集信息,可以通过中继链路的方式收集流经该链路的信息,也可通过和交换机、路由器等网络设备集成收集经这些网络设备转发的信息。二是需要建立攻击特征库,或是描述正常访问过程的行为模式。三是需要设计用于将收集的信息与建立的攻击特征库和描述正常访问过程的行为模式进行比较的匹配操作算法。四是需要设计对攻击信息的反制动作。五是需要分析已经发现的病毒传播过程、木马窃取信息资源过程和黑客利用操作系统漏洞实施的攻击过程,提取出攻击特征,及时添加到攻击特征库中。六是需要不断调整描述正常访问过程的行为模式,在误报和漏报间取得平衡。

5. 简述入侵防御系统防御黑客攻击的机制。

回答：一是通过分析黑客攻击的一般步骤，给出用于描述黑客攻击过程的行为模式（黑客行为模式）。二是对常见黑客攻击方式，如缓冲器溢出攻击、口令穷举攻击等提取出有状态攻击特征，作为黑客攻击特征库中的基本攻击特征。三是不断分析已经发现的黑客攻击行为，提取出攻击特征，及时添加到黑客攻击特征库中。四是针对常用操作系统和应用程序新发现的漏洞，设计黑客可能的攻击行为，在黑客攻击特征库中增加用于描述这些攻击行为的攻击特征。五是在通往重要服务器的链路上设置携带黑客行为模式和黑客攻击特征库的网络入侵防御系统，在重要服务器上设置携带用于检测进出主机信息的攻击特征库的主机入侵防御系统，针对已发现的主机所用操作系统和应用程序漏洞，对主机入侵防御系统设置防止黑客利用漏洞上传并激活蠕虫、篡改和删除重要系统文件的资源访问控制列表。

10.3 实　　验

10.3.1 网络入侵防御系统基本配置实验

1. 实验内容

（1）网络入侵防御系统基本配置。

（2）日志服务器配置。

2. 网络结构

Cisco入侵防御系统和路由器集成在一起，检测机制采用攻击特征检测，反制动作包括丢弃IP分组、通过动态添加过滤规则阻塞攻击源发送的IP分组一段时间和报警等。通过配置，可以将报警消息发送给日志服务器。通过将入侵防御系统作用于路由器接口输入或输出方向，确定该入侵防御系统收集并检测从该路由器接口输入或输出的信息流。

3. 实验步骤

（1）启动Packet Tracer，按照图10.2所示网络结构在逻辑工作区放置和连接设备，放置和连接设备后的逻辑工作区界面如图10.3所示。为路由器接口配置IP地址和子网掩码，同时为终端和日志服务器配置相应的IP地址、子网掩码和默认网关地址。

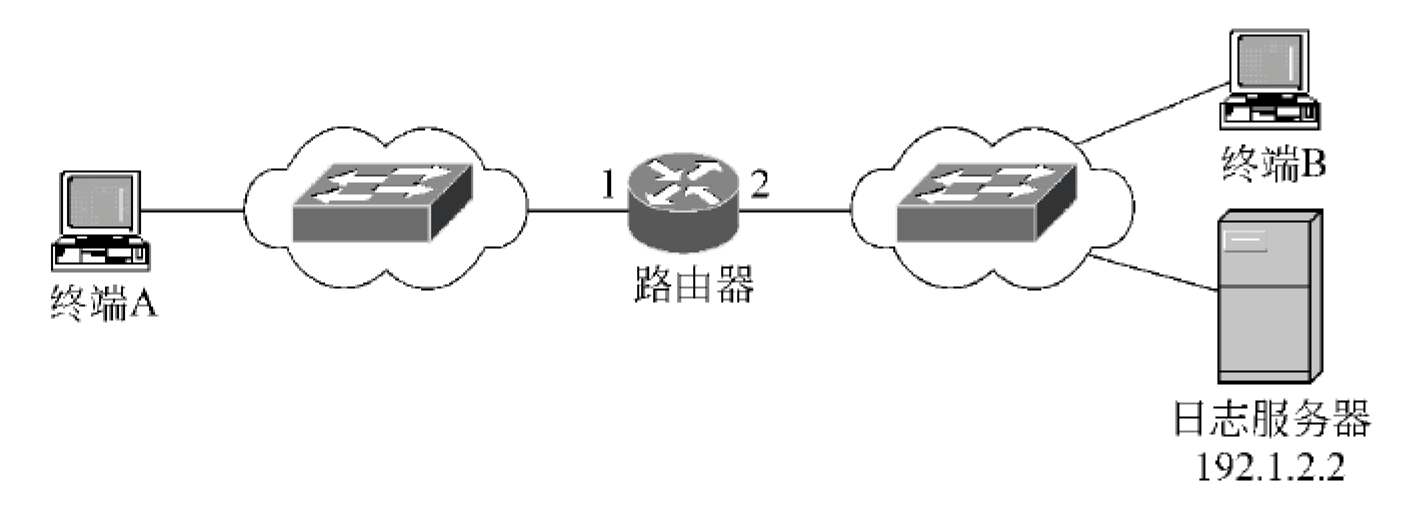


图10.2　网络结构

（2）在路由器flash中创建用于存放攻击特征库的目录flash:\a2，通过命令“ip ips config location flash:\a2”确定路由器启动时将默认攻击特征库加载到目录flash:\a2。

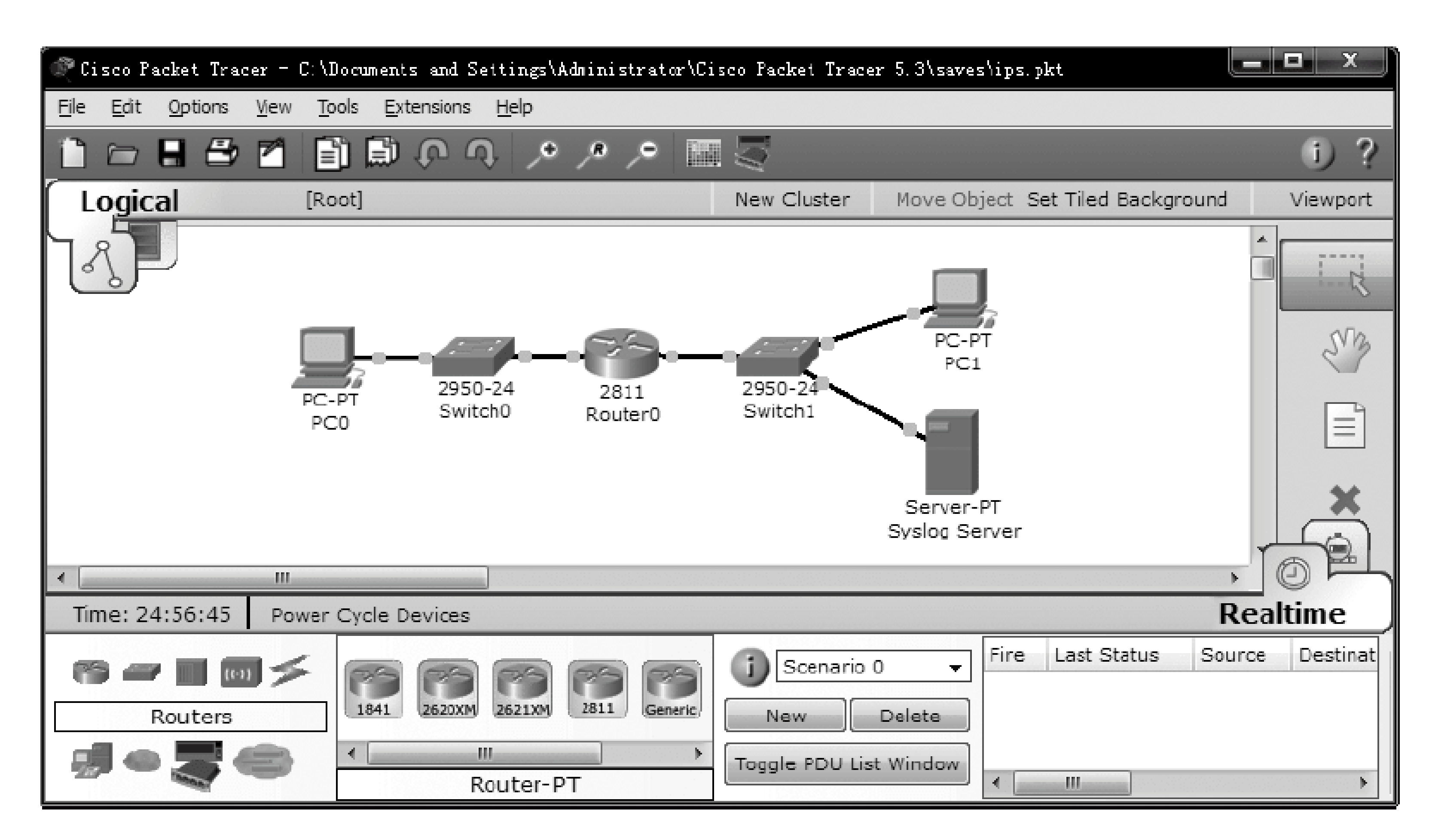


图 10.3　放置和连接设备后的逻辑工作区界面

(3) 通过命令"ip ips name a2"创建名为 a2 的入侵防御系统规则，创建该规则时可以通过定义的扩展分组过滤器指定需要入侵检测的信息流类型。

(4) 通过命令"ip ips signature—category"进入各类攻击特征配置模式，在该配置模式中，通过命令"category all"指定以下配置针对所有攻击特征，在所有攻击特征配置模式下，通过命令"retired false"指定所有攻击特征都不处于隐退状态(非隐退状态)，一旦某类攻击特征处于隐退状态，入侵防御系统检测入侵行为时不对该类攻击特征进行匹配操作。

(5) 通过命令"ip ips notify log"指定向日志服务器发送报警消息，通过命令"logging host 192.1.2.2"指定日志服务器 IP 地址 192.1.2.2，通过命令"logging on"启动发送日志消息过程。

4. 路由器命令行配置过程

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#exit
Router#mkdir flash:\a2                       (在路由器 flash 中创建目录 flash:\a2)
Create directory filename [\a2]?             (按 Enter 键确定创建目录 flash:\a2)
Router#configure terminal
Router(config)#ip ips config location flash:\a2
```

```
                                        (指定存放攻击特征文件的目录 flash:\a2)
Router(config)#ip ips name a2           (创建名为 a2 的入侵防御系统规则)
Router(config)#ip ips notify log        (指定将报警消息发送给日志服务器)
Router(config)#logging host 192.1.2.2   (指定日志服务器 IP 地址 192.1.2.2)
Router(config)#logging on               (启动发送日志消息过程)
Router(config)#ip ips signature-category    (进入攻击特征分类配置模式)
Router(config-ips-category)#category all    (指定所有攻击特征)
Router(config-ips-category-action)#retired false    (指定所有攻击特征处于非隐退状态)
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]      (按 Enter 键确定配置)
Router(config)#ip ips fail closed
                (一旦入侵防御系统无法正常作用,丢弃所有需要入侵检测的信息流类型)
Router(config)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip ips a2 in
                (将名为 a2 的入侵防御规则作用于接口 FastEthernet0/0 输入方向)
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip ips a2 out
                (将名为 a2 的入侵防御规则作用于接口 FastEthernet0/1 输出方向)
Router(config-if)#exit
Router(config)#exit
```

第11章 网络管理和监测

CHAPTER

11.1 知识要点

11.1.1 网络设备配置方式

1. 控制台端口配置方式

交换机和路由器出厂时只有默认配置，如果需要对刚购买的交换机和路由器进行配置，最直接的配置方式是采用图11.1所示的控制台端口配置方式，用串行口连接线互连PC的RS-232串行口和网络设备的控制台(Consol)端口，启动PC的超级终端程序，完成超级终端配置，按Enter键进入网络设备的命令行配置界面。图11.2是Packet Tracer的超级终端配置界面。图11.3是通过超级终端进入的路由器命令行配置界面。

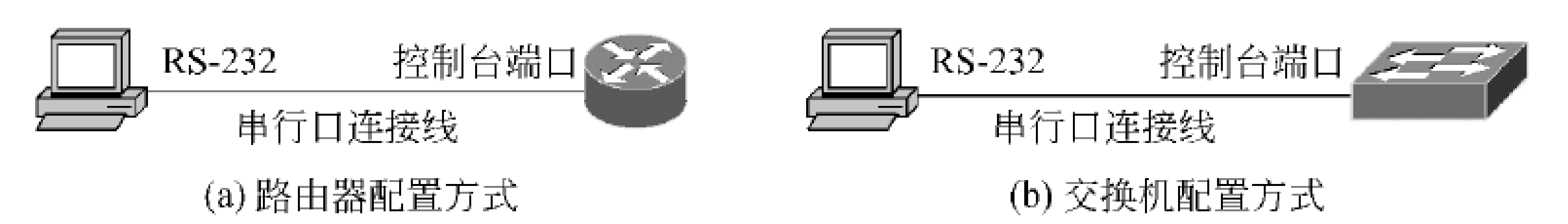


图11.1 控制台端口配置方式

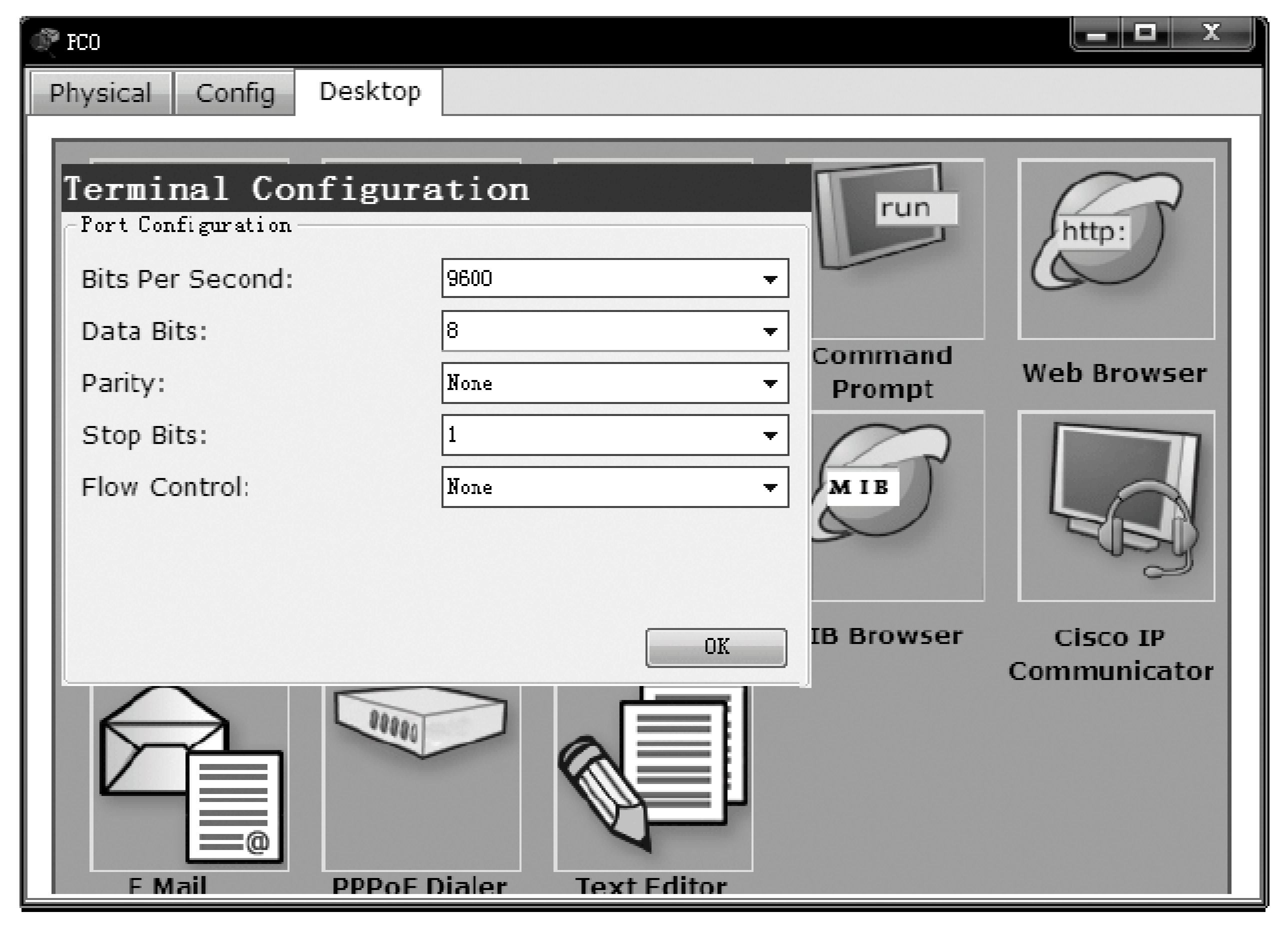


图11.2 超级终端配置界面

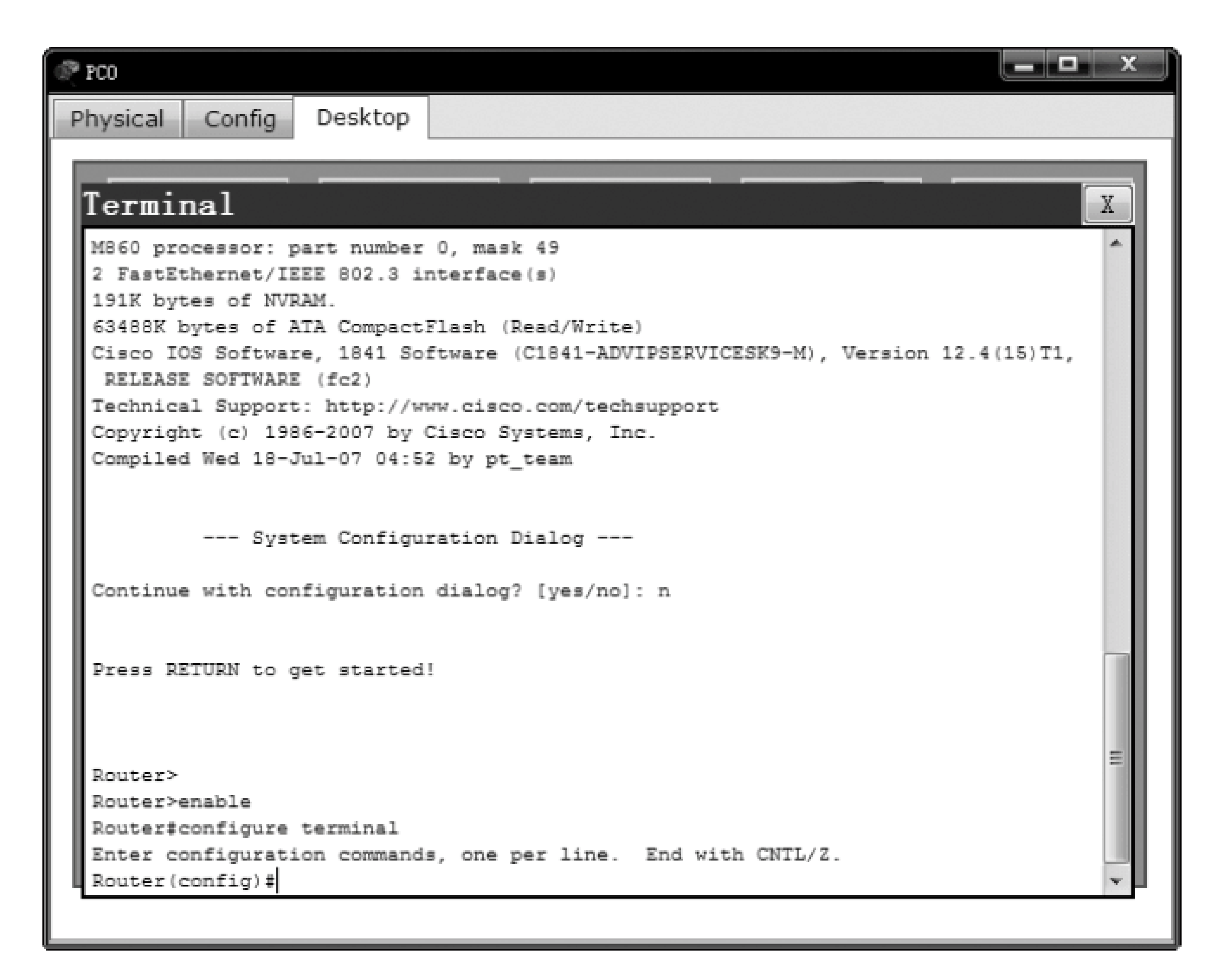


图 11.3　通过超级终端进入的路由器命令行配置界面

一般情况下，通过控制台端口配置方式完成网络设备的基本配置，如交换机管理地址和默认网关地址，路由器各个接口的 IP 地址、静态路由项或路由协议等。其目的是建立终端与网络设备之间的传输通路，只有建立终端与网络设备之间的传输通路，才能通过其他配置方式对网络设备进行配置。

2. Telnet 配置方式

图 11.4 中终端通过 Telnet 配置方式对网络设备实施远程配置的前提是交换机和路由器必须完成图 11.4 所示的基本配置，只有这样，终端和网络设备之间才能相互交换 Telnet 报文。终端一旦通过 Telnet 远程登录网络设备，出现网络设备的命令行配置界面，图 11.5 是终端通过 Telnet 远程登录交换机 S2 后出现的交换机命令行配置界面。

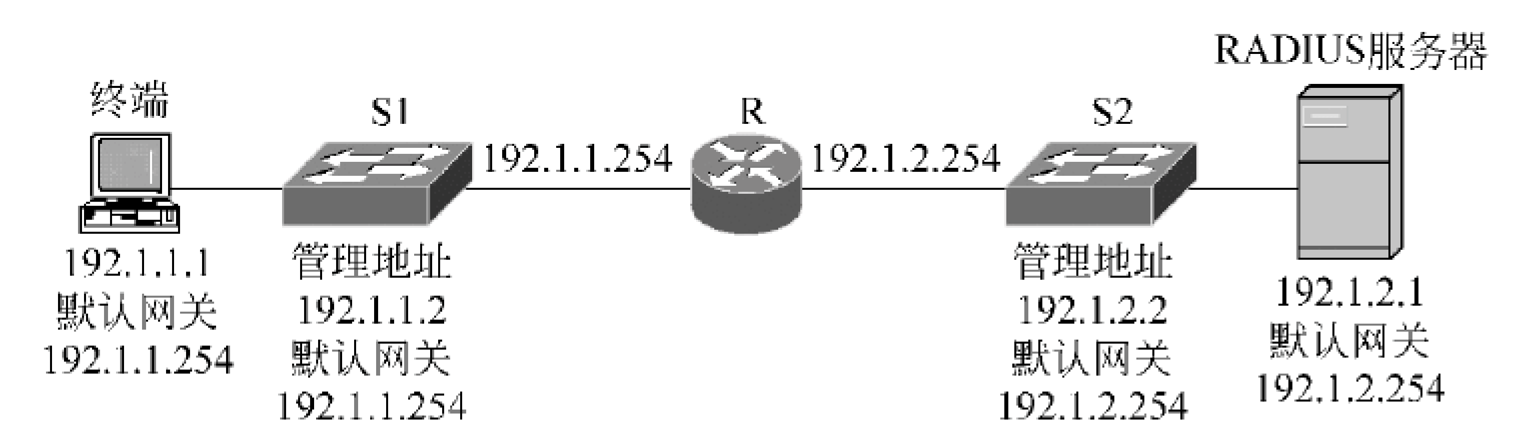


图 11.4　Telnet 配置方式

3. SNMP 配置方式

网络设备可以通过一组对象进行描述，这一组对象的值反映了网络设备的状态和配置，可以通过设置对象的值对网络设备进行配置。简单网络管理协议（Simple Network Management Protocol，SNMP）可以通过＜SET，OID，值＞完成对网络设备某个对象值的设置，其中 SET 是设置命令；OID（Object IDentifier）是对象标识符，用于唯一指定网络设备中的某个对象；值是该对象新设置的值。图 11.6 是 Packet Tracer MIB Browser 设置图 11.4 中交换机 S2 中某个端口状态的值的界面。

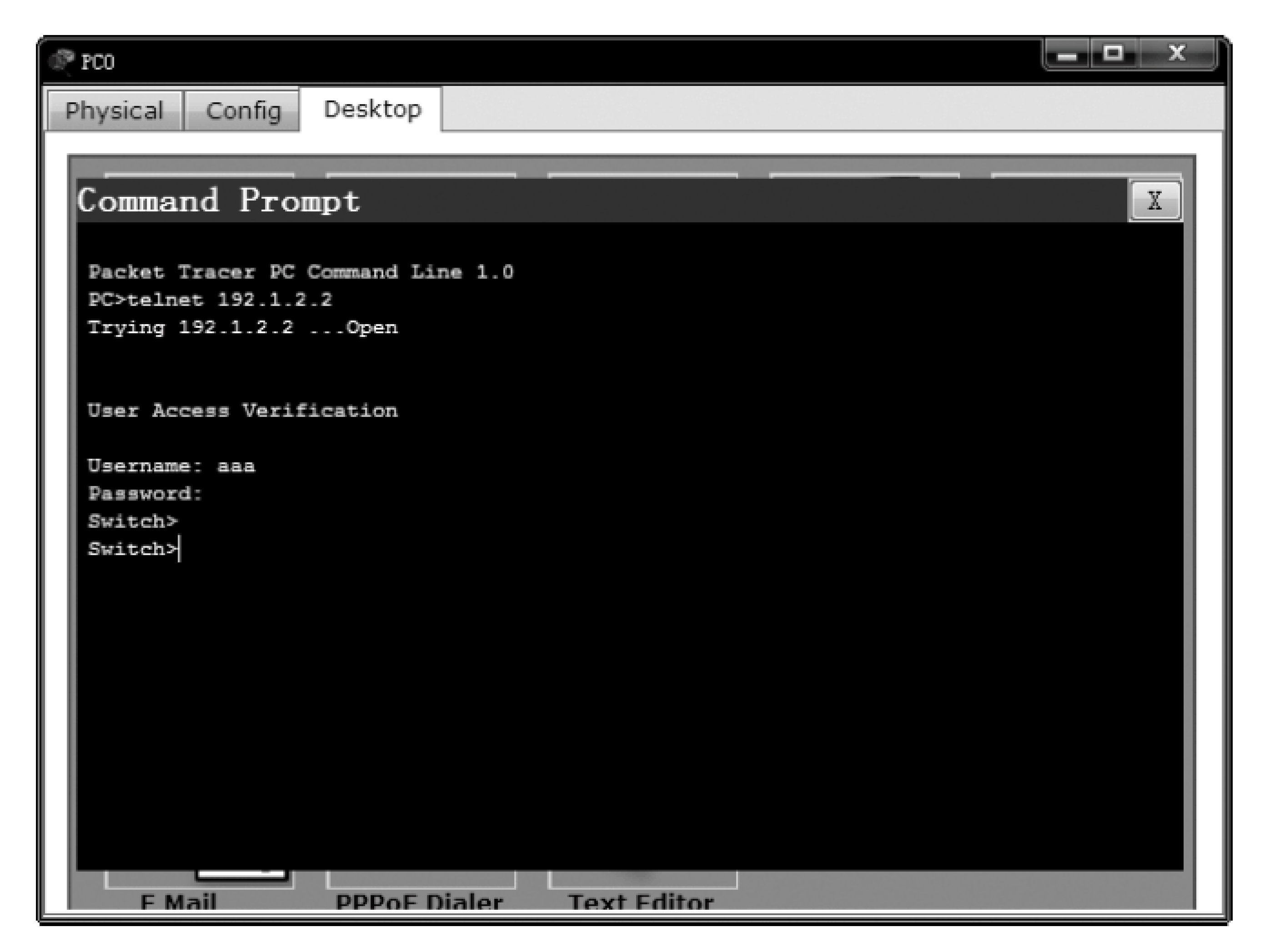


图 11.5　终端远程配置交换机界面

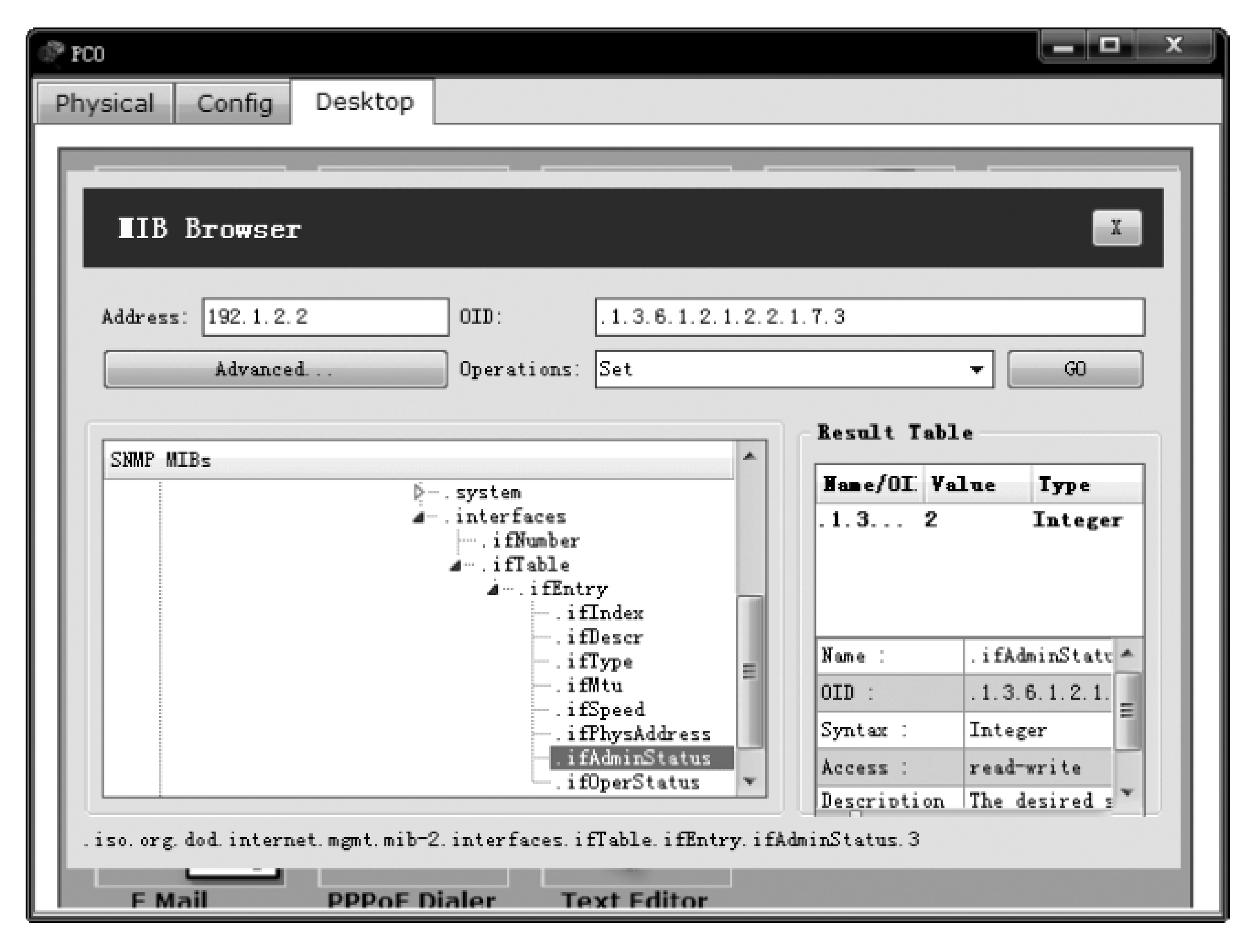


图 11.6　MIB Browser 配置交换机端口状态的界面

11.1.2　SNMP 管理网络过程

1. 网络结构

网络管理是一种通过对硬件、软件和人力的使用、综合和协调，对网络资源的监控、测试、配置、分析和评价，达到以合理的成本满足网络实时性能和服务质量要求的系统。如图 11.7 所示，构成这一系统的主要构件有网络管理工作站和分布在各个网络结点中的管理代理，网络管理工作站通过 SNMP 和分布在各个网络结点中的管理代理交换数据。

管理代理在网络结点中维持网络管理信息库(Management Information Base，MIB)，MIB 是用于描述该网络结点当前状态和配置的一组被管对象的值的集合，通过查询对象

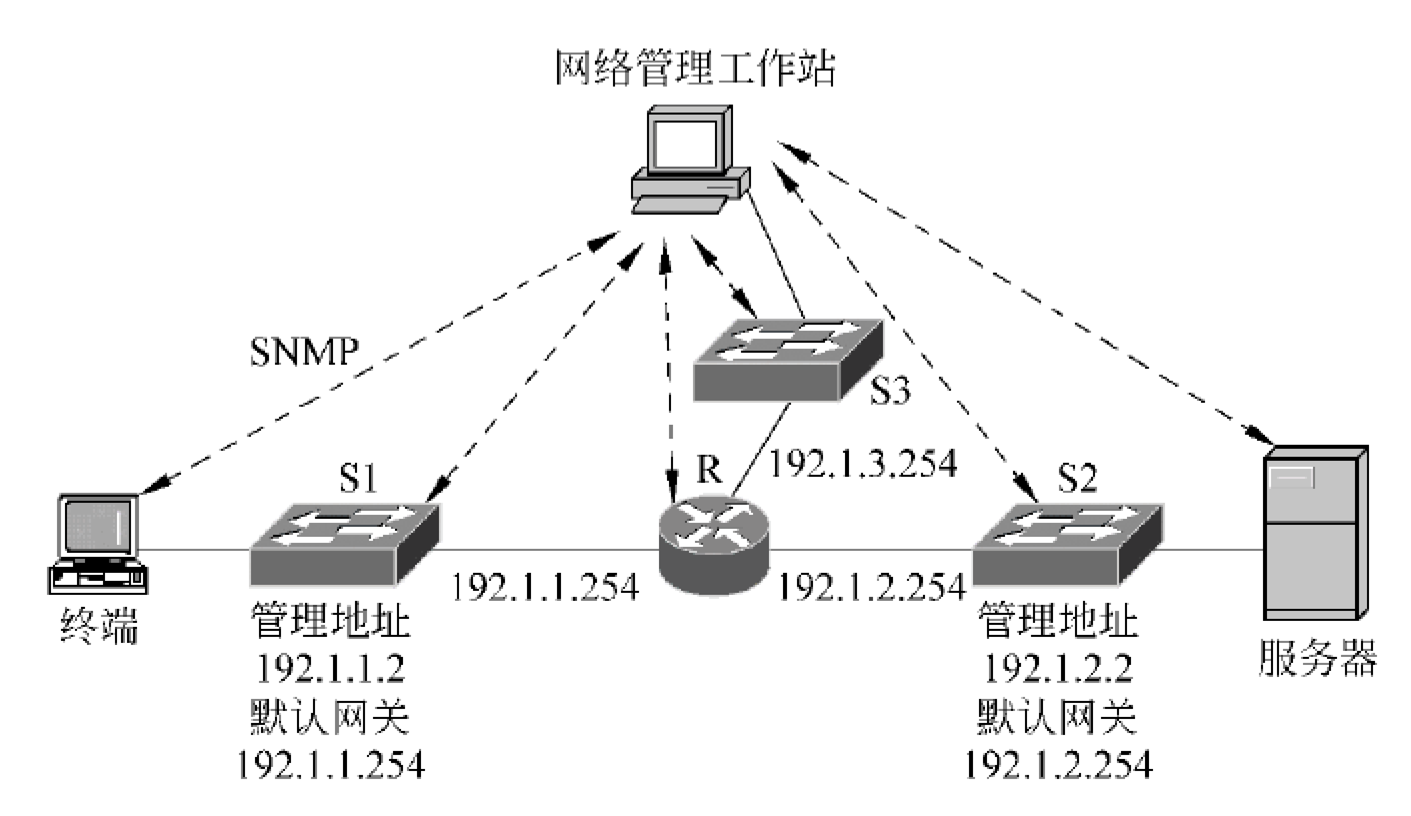


图 11.7 网络结构

的值,网络管理工作站可以获得有关网络的状态,如经过某个路由器接口输出的 IP 分组数、特定终端对之间的流量等。通过设置对象的值,可以对网络结点进行配置,如开启或关闭某个交换机端口。

网络管理工作站和网络结点中管理代理、被管对象和 MIB 之间关系如图 11.8 所示。网络管理工作站通过 SNMP 与管理代理交换数据,管理代理一方面采集被管对象的信息(如经过某个路由器接口输出的 IP 分组数)并将其存储到 MIB 中;另一方面通过修改 MIB 中某个被管对象关联的值(如某个交换机端口的状态值),改变被管对象的配置(如开启或关闭该交换机端口)。

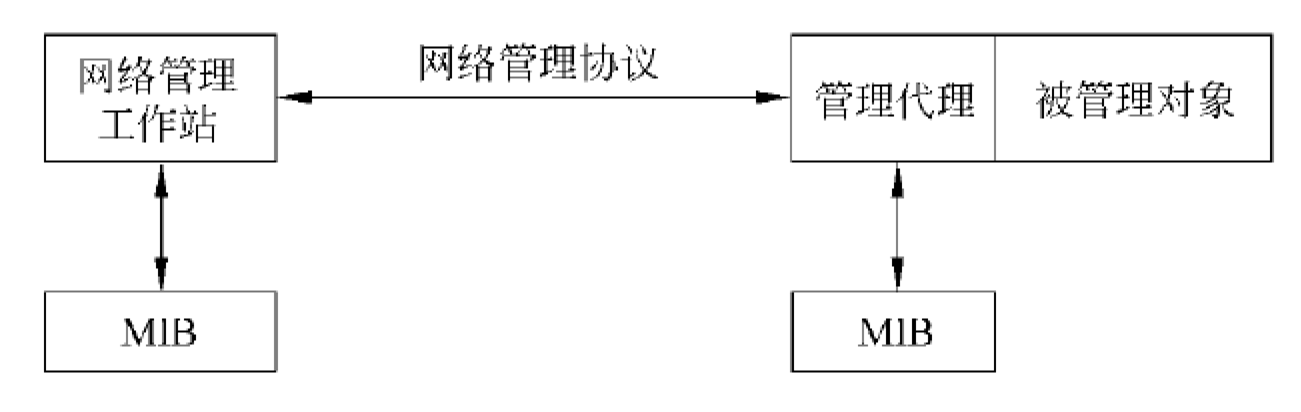


图 11.8 网络管理系统结构

2. SMI 和 MIB

每一个网络结点,如交换机和路由器,可以被分解为多个被管对象。被管对象可以是构成该网络结点的其中一个硬件构件,如路由器接口、交换机端口等;也可以是网络协议,如路由器中的路由协议 RIP 和 OSPF 等。与被管对象关联的参数值构成 MIB。

管理信息结构(Structure of Management Information,SMI)的主要功能是规定被管对象命名方式、定义被管对象数据类型和制定被管对象与值的编码规则。SMI 规定所有被管对象必须处于被管对象树上。图 11.9 是交换机对应的被管对象树,树结构中的每一个对象都有相应的标号,如 iso 的标号为 1,每一个被管对象用树根至被管对象分枝经过的所有对象的标号的组合作为其对象标识符,如被管对象 iso. org. dod. internt. mgmt. mib-2. interface. ifTable. ifEntry. ifType 的对象标识符为 1. 3. 6. 1. 2. 1. 2. 2. 1. 3。SMI 定义的基本数据类型如表 11.1 所示。每一个被管对象分配一种 SMI 定义的数据类型,如被管对象 iso. org. dod. internt. mgmt. mib-2. interface. ifTable. ifEntry. ifType 的数据类型为 INTEGER。

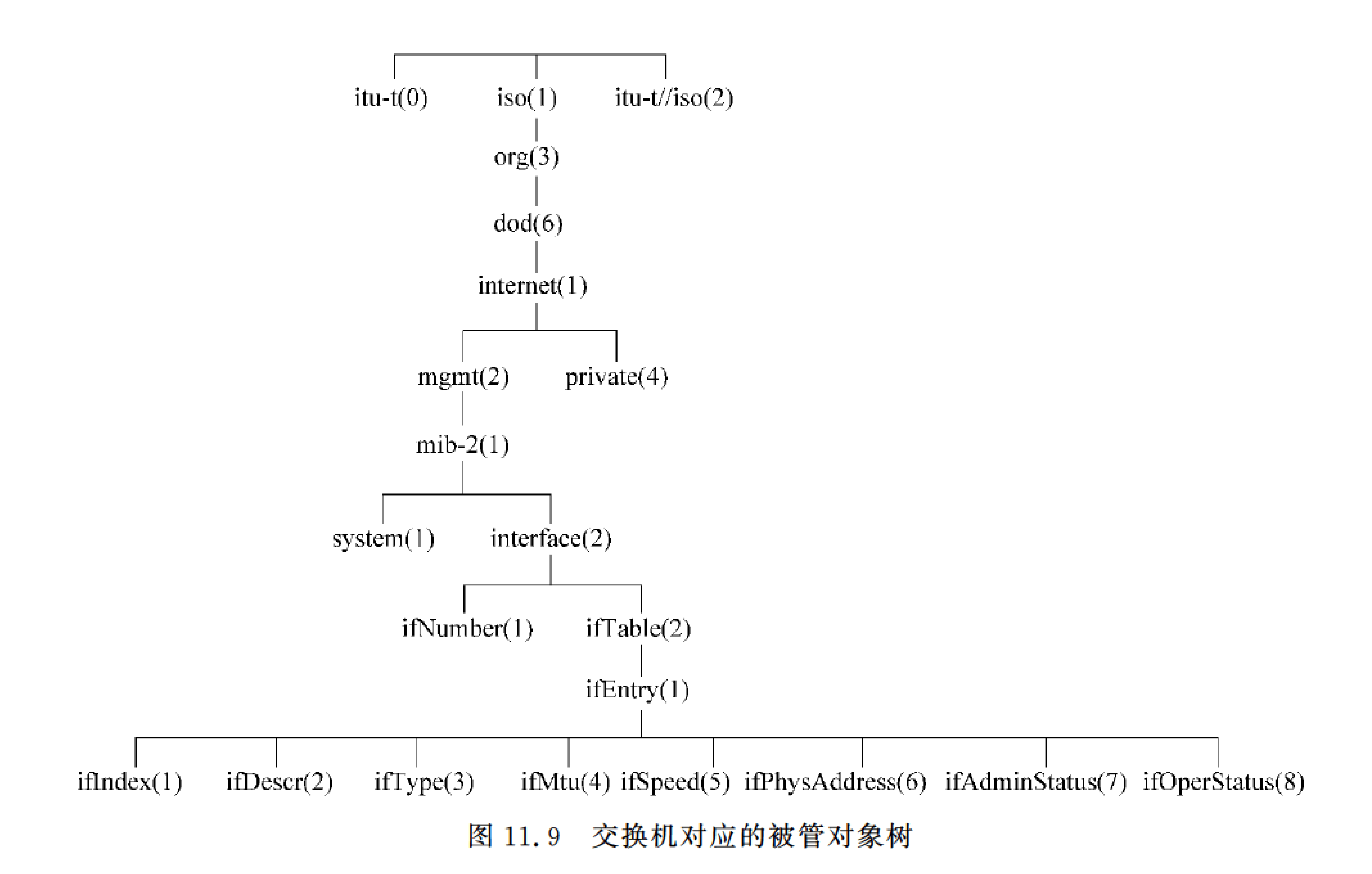


图 11.9　交换机对应的被管对象树

表 11.1　SMI 定义的基本数据类型

数据类型	描　　述
INTEGER	32 位整数，其值范围为 $-2^{31}\sim2^{31}-1$
Integer32	32 位整数，其值范围为 $-2^{31}\sim2^{31}-1$
Unsigned32	32 位无符号整数，其值范围为 $0\sim2^{32}-1$
OCTET STRING	ASN.1 格式字节串，表示任意二进制或文本数据，最大长度为 65 535
OBJECT IDENTIFIER	对象标识符
IPAddress	32 位 IP 地址
Counter32	32 位计数器，从 0 增加到 $2^{32}-1$，然后回归到 0
Counter64	64 位计数器
Gauge	32 位计量器，计量范围为 $0\sim2^{32}-1$
TimeTicks	记录时间的计数器，以 1/1000s 为单位
BITS	比特串
Opaque	不解释的串

不同网络设备有着不同的 MIB，SMI 不会对每一种网络设备 MIB 中被管对象的组成作出规定，但每一种网络设备 MIB 中的被管对象必须构成 SMI 规定的对象树，每一个被管对象必须处于对象树上，被管对象标识符的命名方式必须使用 SMI 规定的命名方式，每一个被管对象必须属于 SMI 定义的数据类型。

11.2 例题解析

11.2.1 自测题

1. 选择题

(1) 下述________配置方式不适合用于刚出厂的网络设备。

A. 控制台端口配置方式　　B. 一对一 Telnet 配置方式

C. 一对一 Web 配置方式　　D. Telnet 在线配置方式

(2) 下述________是 SNMP 有别于 Telnet 的地方。

A. 配置网络设备　　B. 查询网络设备状态

C. 单台终端在线配置多个网络设备　　D. 网络设备主动报告发生的事件

(3) 下述________不是采用命名对象树的好处。

A. 方便给出唯一标识对象的对象标识符

B. 体现对象之间的层次关系

C. 方便增加对象

D. 需要在合适的结点下注册对象

(4) 下述________是 SNMPv1 验证网络管理员权限的机制。

A. 公共体　　B. 对称密钥　　C. 证书　　D. 数字签名

(5) 下述________是 SNMPv3 验证网络管理员身份的机制。

A. 公共体　　B. 对称密钥　　C. 证书　　D. 数字签名

(6) 下述________与 SNMPv3 确定访问权限无关。

A. 公共体　　B. 对称密钥　　C. 用户名　　D. 安全等级

(7) 下述________不是 SNMP 网络管理系统特有的功能。

A. 提供网络全局视图　　B. 主动报警

C. 广泛的被管对象　　D. 网络设备配置

(8) 下述________不是网络管理工作站的功能。

A. 查询被管对象状态　　B. 设置被管对象状态

C. 综合从被管对象收集到的信息　　D. 出厂网络设备的初始配置

(9) 下述________不是 SMI 的功能。

A. 规定被管对象命名方式　　B. 定义被管对象数据类型

C. 制定被管对象和值的编码规则　　D. 指定网络设备被管对象组成和结构

(10) 下述关于 MIB 的描述________是错误的。

A. 被管对象值的集合构成 MIB　　B. 查询是读取指定被管对象的值

C. 设置是写入指定被管对象的值　　D. 所有网络设备有着相同的 MIB

2. 填空题

(1) 网络管理功能主要包括________、________、________、________和________。

(2) SNMPv1 中被管设备通过________确定网络管理员权限，SNMPv1 用________传输________，因此，极易被黑客嗅探或截获，导致黑客具有管理该被管设备的权限。

(3) SNMPv3 中被管设备通过________鉴别网络管理员身份，通过________、________和________确定网络管理员权限，由于可以________传输________，导致黑客无法嗅探被管设备状态。

(4) SMI 的功能包括________、________和________。

(5) 不同网络设备具有________的 MIB，网络设备中的代理只能读写________的被管对象的值。但必须用________规定的被管对象命名方式命名 MIB 中的被管对象，MIB 中被管对象类型只能是________定义的被管对象数据类型。

(6) 网络管理系统包括________、________、________、________和________等主要构件。

(7) SNMP 用________命令读取 MIB 中的值，用________命令设置 MIB 中的值，网络管理员如果要设置 MIB 中的值，表示网络管理员拥有的公共体具有________的权限。

(8) SNMP 存在两种获得被管对象状态的方式，它们是________和________。

(9) 图 11.9 中被管对象 ifSpeed 的对象标识符是________，如果需要在图 11.9 中增加 Cisco 和 3com 特有的被管对象，应该在结点________下增加结点 enterprises，在结点 enterprises 下增加结点________和________。

3. 名词解释

____网络管理协议	____ SNMPv3
____被管设备	____被管对象
____网络管理工作站	____管理代理
____ SMI	____ MIB

(a) 运行网络管理程序的主机，运行的网络管理程序实现通过网络管理协议查询和设置被管对象状态，对收集到的被管对象信息进行综合分析和处理，向管理员提供网络全局视图的功能。

(b) 一种集成在被管设备中，维持 MIB，通过网络管理协议和网络管理工作站通信，并根据网络管理工作站的要求查询和设置被管对象状态的代理程序。

(c) 一种由网络管理工作站实施管理的网络设备，如交换机、路由器和主机等。

(d) 构成被管设备的构件，可以是被管设备的某个硬件构件，如接口；也可以是被管设备运行的某个协议软件，如 RIP。

(e) 管理信息结构，其功能包括规定被管对象命名方式、定义被管对象数据类型和制定被管对象与值的编码规则。

(f) 管理信息库，被管对象的值的集合。

(g) 一种用于实现网络管理工作站和管理代理之间通信的协议。

(h) 简单网络管理协议的最新版本，增加了基于用户管理授权和安全传输 SNMP 报文的功能。

4. 判断题

(1) 网络管理系统的核心功能是配置网络设备。

(2) 一对一 Telnet 配置和一对一浏览器配置可以取代控制台端口配置方式。

(3) 在线 Telnet 配置的前提是已经实现终端和设备之间的数据通信功能。

(4) SMI定义的对象树可以方便增加被管对象。

(5) 安全传输SNMP报文是非常重要的。

(6) 不同网络设备对应不同的MIB。

(7) 企业可以自己定义MIB,但必须注册在SMI定义的对象树的某个结点下,MIB对应的被管对象全部处于对象树该结点下的某个分枝上。

(8) SNMP是实现网络管理程序和被管设备中的管理代理之间通信的协议。

(9) SNMPv3采用共享对称密钥鉴别机制。

(10) SNMPv3用一个口令生成用于与多个不同的被管设备安全通信的多个不同的密钥。

11.2.2 自测题答案

1. 选择题答案

(1) D,Telnet在线配置的前提是已经建立终端与网络设备之间的传输通路,这是网络设备的默认配置所无法实现的。

(2) D,陷阱和通知机制是SNMP特有的。

(3) D,这一点没有带来方便性。

(4) A,网络设备通过匹配公共体来验证管理员对被管对象的读写权限。

(5) B,用户通过表明拥有指定对称密钥来证明自己身份。

(6) A,SNMPv3不再使用公共体。

(7) D,网络设备配置是Telnet和控制台端口配置方式也具有的功能。

(8) D,这通常是控制台端口配置方式具有的功能。

(9) D,SMI不涉及不同网络设备被管对象的组成。

(10) D,不同网络设备有着不同的MIB。

2. 填空题答案

(1) 故障管理,计费管理,配置管理,性能管理,安全管理。

(2) 公共体,明文,公共体。

(3) 共享密钥,用户名,安全模型,安全级别,加密,SNMP报文。

(4) 规定被管对象命名方式,定义被管对象数据类型,制定被管对象和值的编码规则。

(5) 不同,MIB包含,SMI,SMI。

(6) 网络管理工作站,网络管理协议,管理代理,MIB,被管对象。

(7) GET,SET,读写该被管对象,

(8) 查询,通知。

(9) 1.3.6.1.2.1.2.2.1.5,private,Cisco,3com。

3. 名词解释答案

g	网络管理协议	h	SNMPv3
c	被管设备	d	被管对象
a	网络管理工作站	b	管理代理
e	SMI	f	MIB

4. 判断题答案

(1) 错，配置网络设备是网络管理系统的其中一个功能，和其他功能相比，该功能的重要性并不突出。

(2) 对，有些网络设备有着默认的管理地址，且默认方式下允许用该管理地址远程登录，或访问 Web 页面，因此可以用一台终端直接连接一台网络设备的方式(一对一方式)对该网络设备进行配置。

(3) 对，否则无法远程登录网络设备。

(4) 对，可以自定义对象树，然后将自定义的对象树作为分枝注册到某个结点下。

(5) 对，SNMP 报文中包含网络设备的状态和设置网络设备的命令。

(6) 对，不同网络设备由不同的被管对象组成。

(7) 对，通过这种方式，很方便地增加被管对象。

(8) 对，SNMP 是一种实现网络管理程序和被管设备中的管理代理之间通信的网络管理协议。

(9) 对，SNMPv3 中每一个用户有着用户名和口令，用口令和被管设备标识符产生和该被管设备之间的共享对称密钥，通过共享密钥证明用户拥有口令。

(10) 对，SNMPv3 用口令和被管设备标识符产生和该被管设备之间的共享密钥。由于不同的被管设备有着不同的设备标识符，因此针对不同的被管设备产生的共享密钥也不同。

11.2.3　简答题解析

1. 简述控制台端口配置方式不可替代的原因。

回答：虽然网络设备出厂时有默认的管理地址，但通过默认配置无法建立起终端与网络设备之间的数据传输通路，因此需要通过控制台端口配置方式完成基本配置，基本配置必须保证终端与需要远程配置的网络设备之间的连通性。有些网络设备默认方式下允许用默认管理地址远程登录，或访问 Web 页面，因此可以用一台终端直接连接一台网络设备的方式(一对一方式)对该网络设备进行配置。但这种配置只能算是控制台端口配置方式的变种。

2. 简述 Telnet 和 SNMP 管理网络设备的方式。

回答：Telnet 远程登录网络设备后，可以通过终端输入所有网络设备支持的命令。SNMP 可以通过 SET 命令对被管对象设置新值，但要求一是被管对象必须是该网络设备 MIB 包含的被管对象，二是该被管对象必须是可读写的。

3. 简述采用对象命名树的原因。

回答：一是方便命名被管对象，二是方便增加被管对象，三是方便体现被管对象的层次结构。

11.3　实　　验

11.3.1　控制台端口方式配置网络设备实验

1. 实验内容

(1) 完成终端 RS-232 串行口和网络设备控制台端口之间的连接。

(2) 配置超级终端。

(3) 通过超级终端进入网络设备命令行配置界面。

2. 网络结构

网络结构如图 11.1 所示。用串行口连接线互连终端 RS-232 串行口和网络设备控制台端口。每一个终端每一次连接一台网络设备,因此,控制台端口配置方式需要逐台连接、逐台配置网络设备。

3. 实验步骤

(1) 启动 Packet Tracer,在逻辑工作区根据图 11.1 所示的网络结构放置和连接设备,逻辑工作区完成设备放置和连接后的界面如图 11.10 所示。

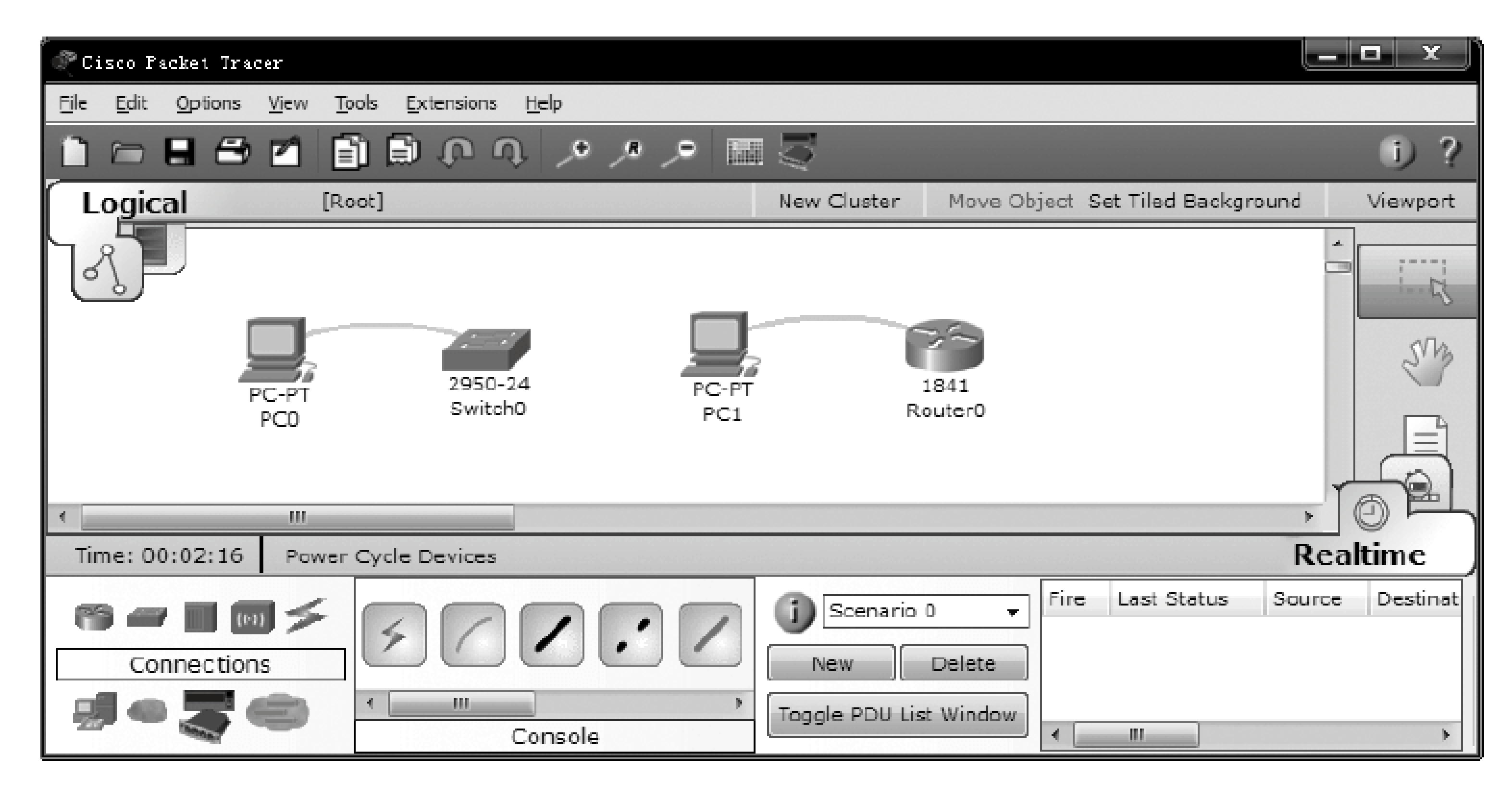


图 11.10 放置和连接设备后的逻辑工作区界面

(2) 启动桌面中的终端(Terminal)程序,出现图 11.11 所示的终端配置界面,单击 OK 按钮,进入网络设备命令行配置界面。图 11.12 所示是交换机命令行配置界面。图 11.13 所示是路由器命令行配置界面。

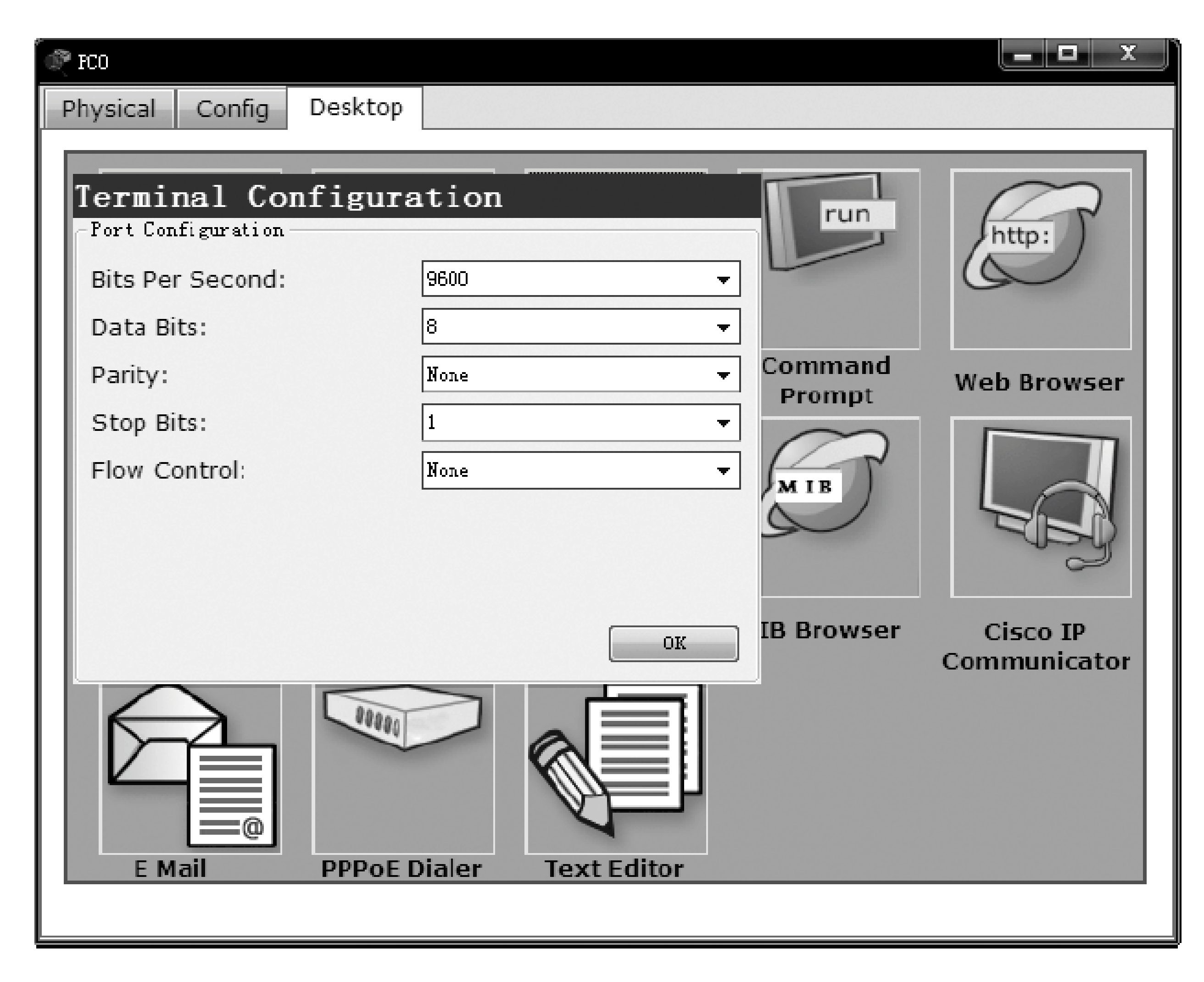


图 11.11 终端配置界面

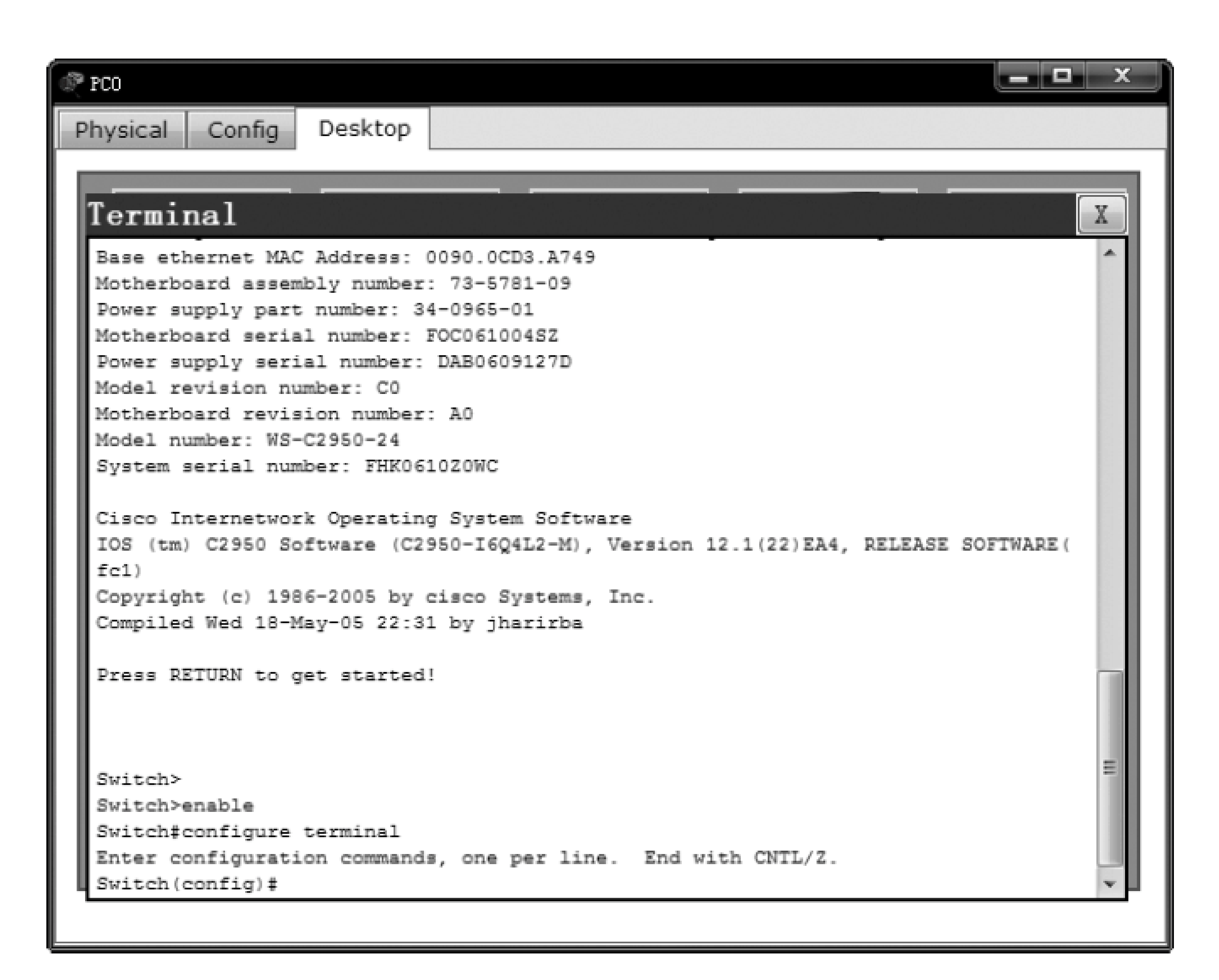


图 11.12　通过终端程序进入的交换机命令行配置界面

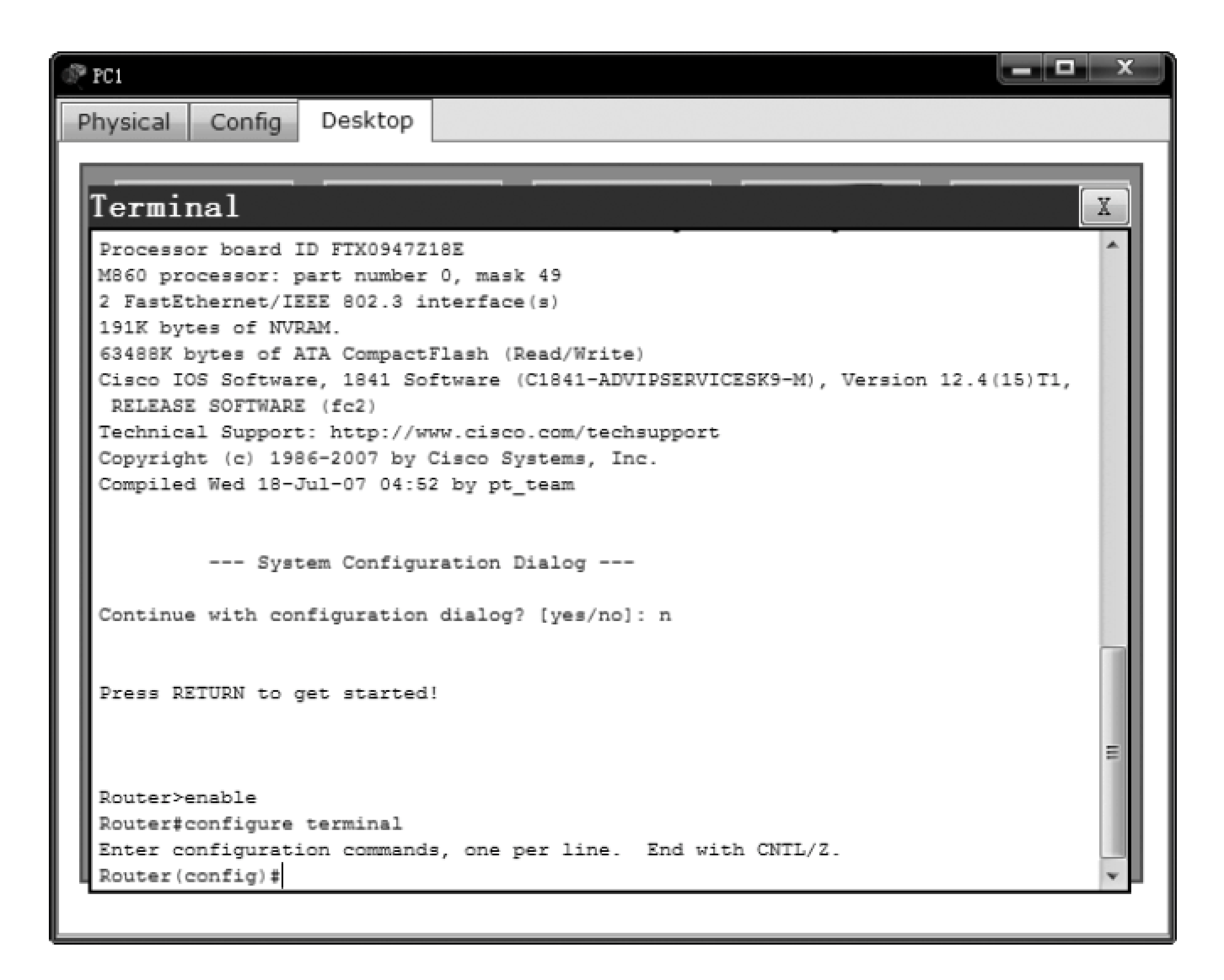


图 11.13　通过终端程序进入的路由器命令行配置界面

11.3.2　Telnet 方式配置网络设备实验

1. 实验内容

（1）完成网络设计。

（2）完成交换机配置。

（3）完成路由器配置。

（4）完成 RADIUS 服务器配置。

2. 网络结构

网络结构如图 11.4 所示。首先必须为交换机配置管理地址，这里，交换机管理地址选择 VLAN 1 的 IP 接口地址，因此该地址必须属于分配给 VLAN 1 的网络地址。同时需要配置默认网关地址，该地址是路由器连接 VLAN 1 的接口的 IP 地址。通过 Telnet 远程登录网络设备时，需要验证登录用户身份，存在三种验证登录用户身份机制：一是在线路配置模式设置口令，远程登录网络设备时，必须输入该口令。二是在线路配置模式选择用本地用户库验证登录用户身份，同时在全局配置模式创建本地用户，远程登录网络设备时，必须输入某个本地用户的用户名和口令。三是在网络中配置 RADIUS 服务器，在 RADIUS 服务器中创建用户，在路由器中指定使用 RADIUS 服务器中的用户信息验证登录用户的身份，远程登录网络设备时，必须输入某个 RADIUS 服务器中创建的用户的用户名和口令。图 11.4 中交换机 S1 使用口令鉴别机制，交换机 S2 使用本地用户库鉴别机制，路由器 R 使用 RADIUS 服务器鉴别机制。网络设备必须设置 ENABLE 口令，否则远程登录网络设备后，用户优先级是最低级，大多数命令无法使用。

3. 实验步骤

(1) 启动 Packet Tracer，在逻辑工作区根据图 11.4 所示的网络结构放置和连接设备，逻辑工作区完成设备放置和连接后的界面如图 11.14 所示。

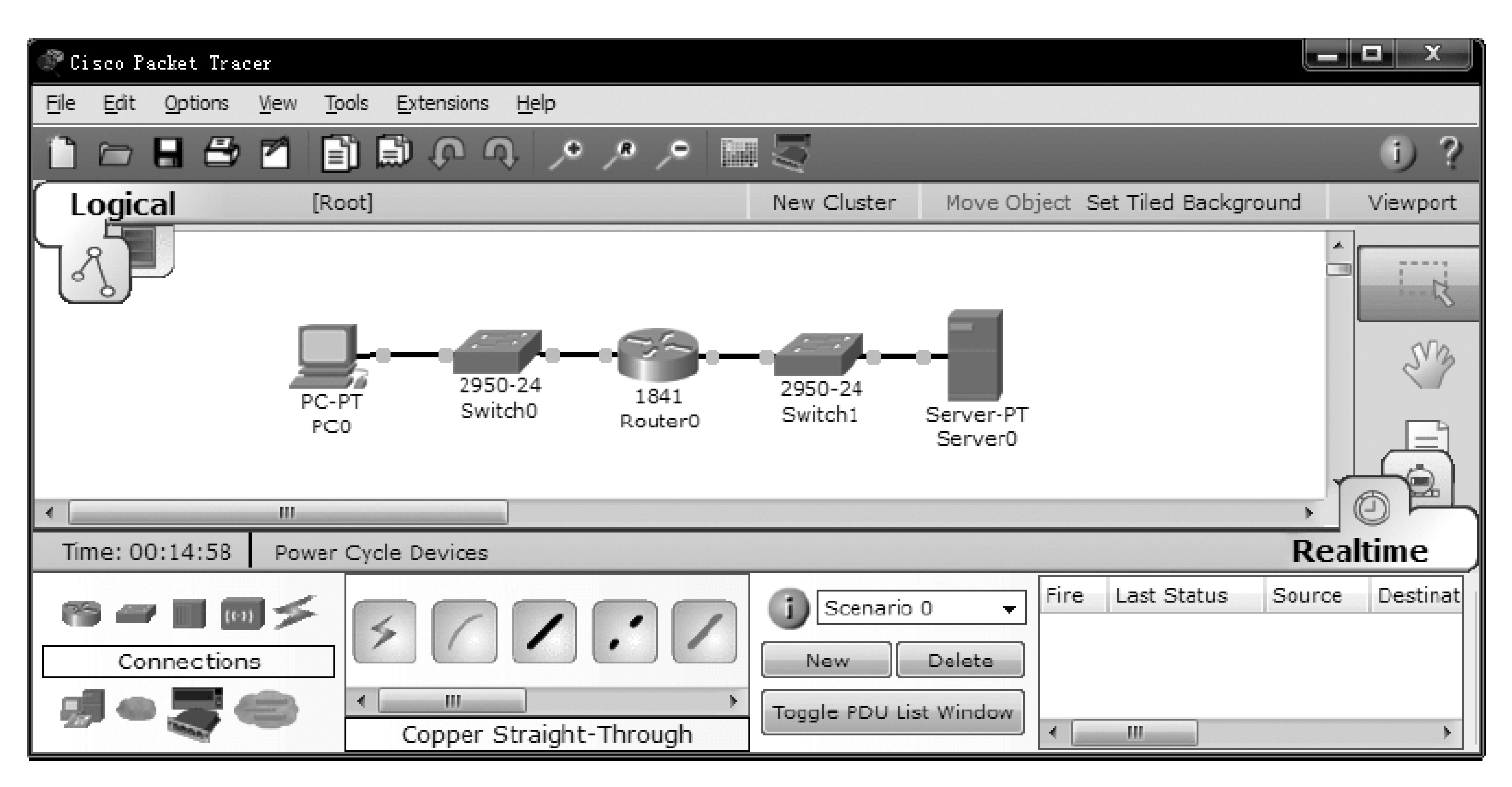


图 11.14 放置和连接设备后的逻辑工作区界面

(2) 为路由器接口配置 IP 地址和子网掩码，为交换机配置管理地址和默认网关地址。由于所有交换机端口属于 VLAN 1，交换机配置的管理地址必须属于连接该交换机的路由器接口的 IP 地址和子网掩码所确定的网络地址，默认网关地址是该路由器接口的 IP 地址。

(3) Switch0 在线路配置模式下通过命令 password abc 确定用口令 abc 作为鉴别远程登录用户身份的鉴别信息。Switch1 在线路配置模式下通过命令 login local 确定使用本地用户信息作为鉴别远程登录用户身份的鉴别信息。同时在全局配置模式下通过命令 username aaa password bbb 创建用户名为 aaa，口令为 bbb 的本地用户。Router0 首先在全局配置模式下通过命令 aaa authentication login a1 group radius 创建名为 a1 的远程登录鉴别机制，该机制通过 RADIUS 服务器验证登录用户身份。在线路配置模式下通过命令 login authentication a1 确定使用名为 a1 的远程登录鉴别机制鉴别登录用户身份。在

全局配置模式下通过命令“radius－server host 192.1.2.1”指定 RADIUS 服务器 IP 地址是 192.1.2.1，通过命令“radius－server key 1234”指定 Router0 与 RADIUS 服务器交换 RADIUS PDU 时使用的密钥 1234。因此，在配置 RADIUS 服务器时，需要给出 Router0 的主机名 Router，Router0 向 RADIUS 服务器发送 RADIUS PDU 时使用的 IP 地址 192.1.2.254，RADIUS 服务器与 Router0 交换 RADIUS PDU 时使用的密钥 1234。同时，创建名为 ccc，口令为 ddd 的用户。RADIUS 服务器配置界面如图 11.15 所示。

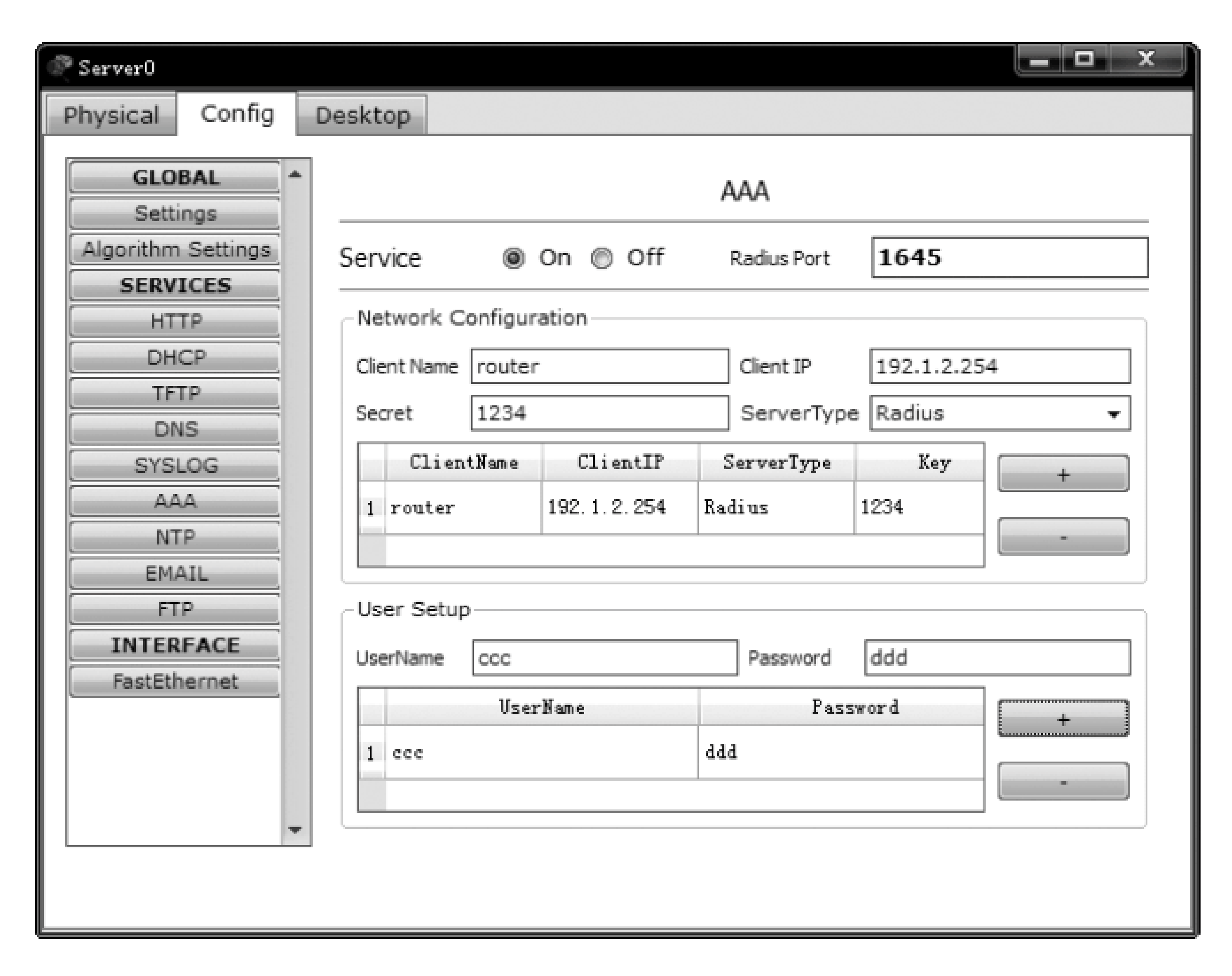


图 11.15　RADIUS 服务器配置界面

（4）完成上述配置后，PC0 可以 Telnet 远程登录网络设备。图 11.16 是 PC0 远程登录 Switch0 的界面。图 11.17 是 PC0 远程登录 Switch1 的界面。图 11.18 是 PC0 远程登录 Router0 的界面。

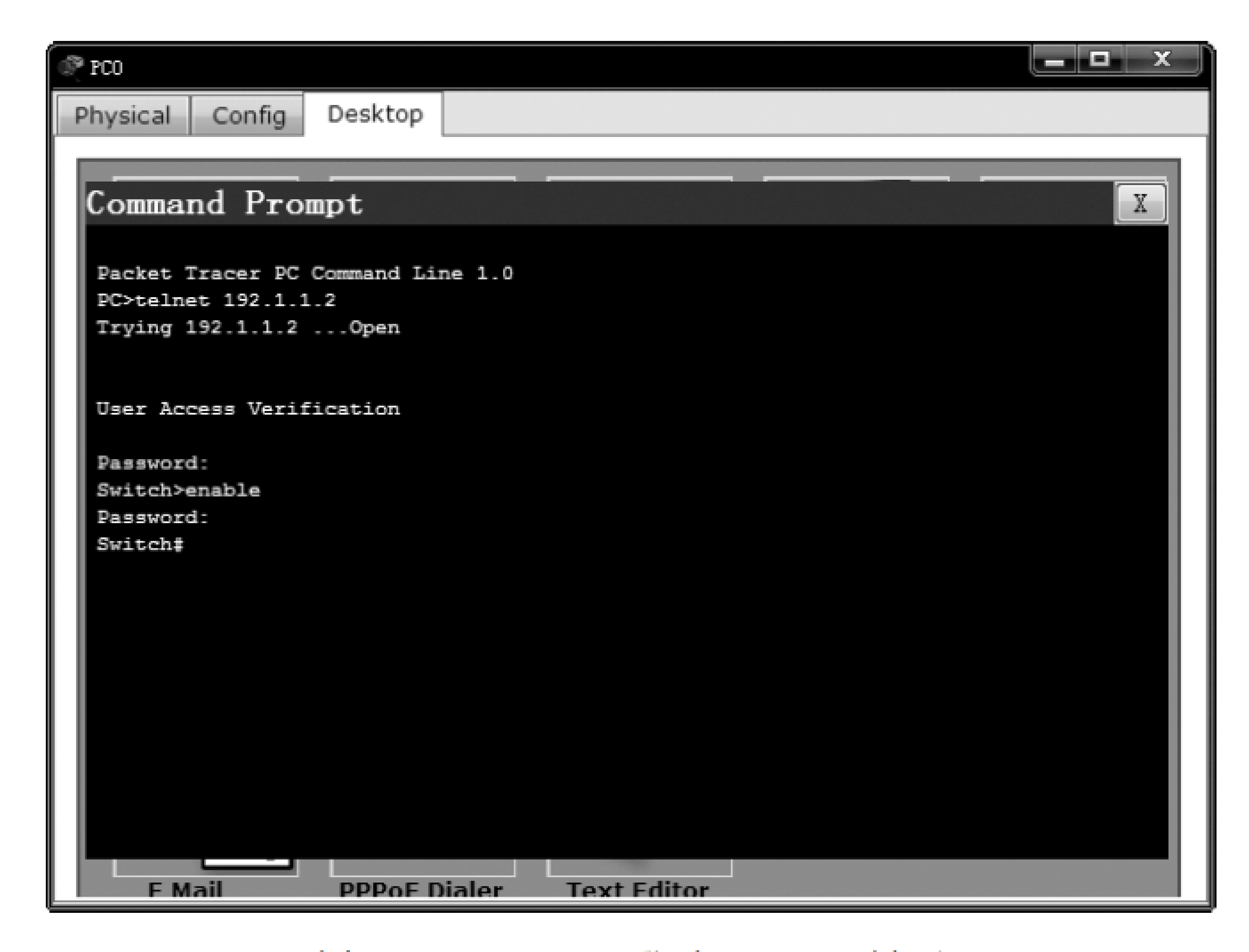


图 11.16　Telnet 登录 Switch0 界面

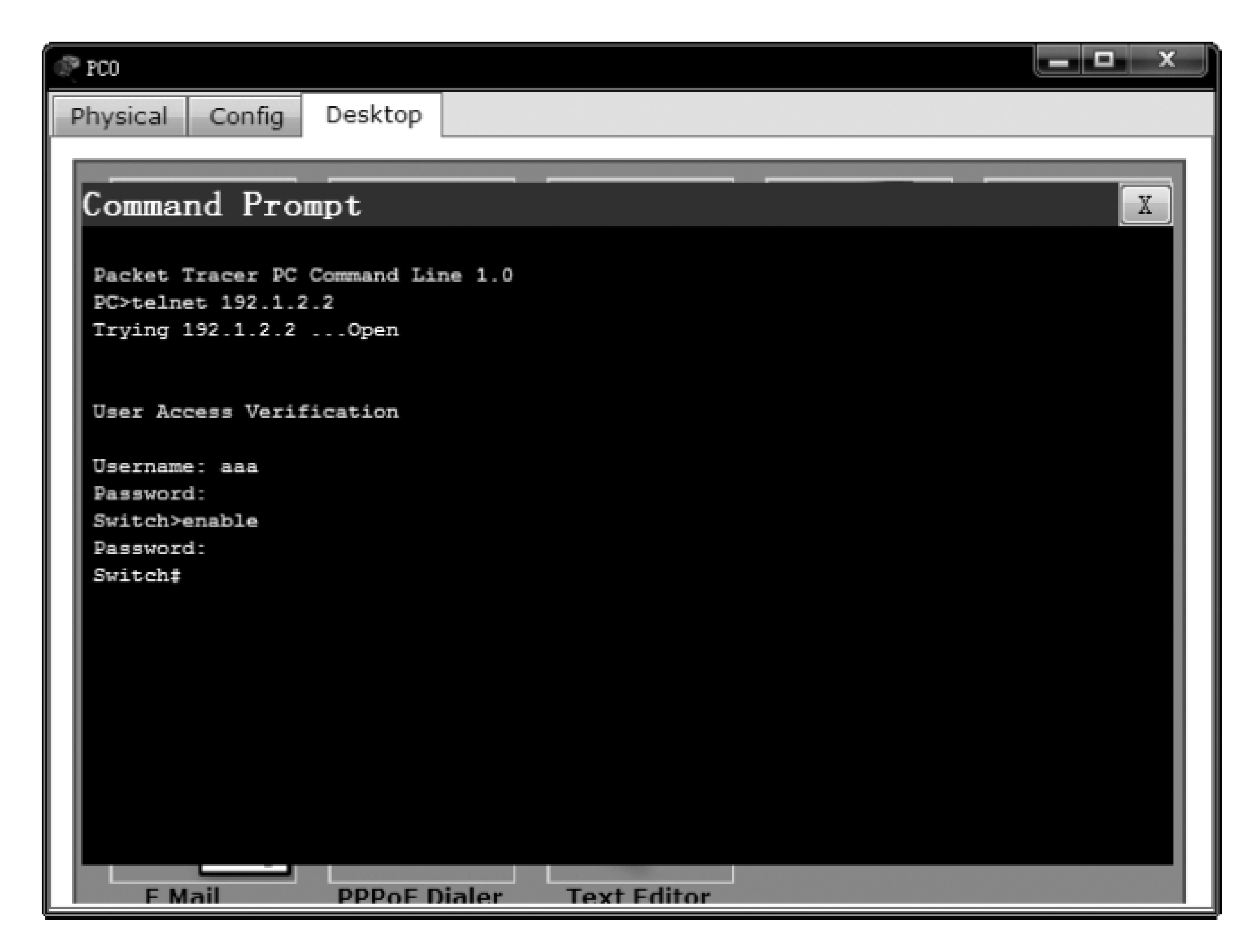


图 11.17 Telnet 登录 Switch1 界面

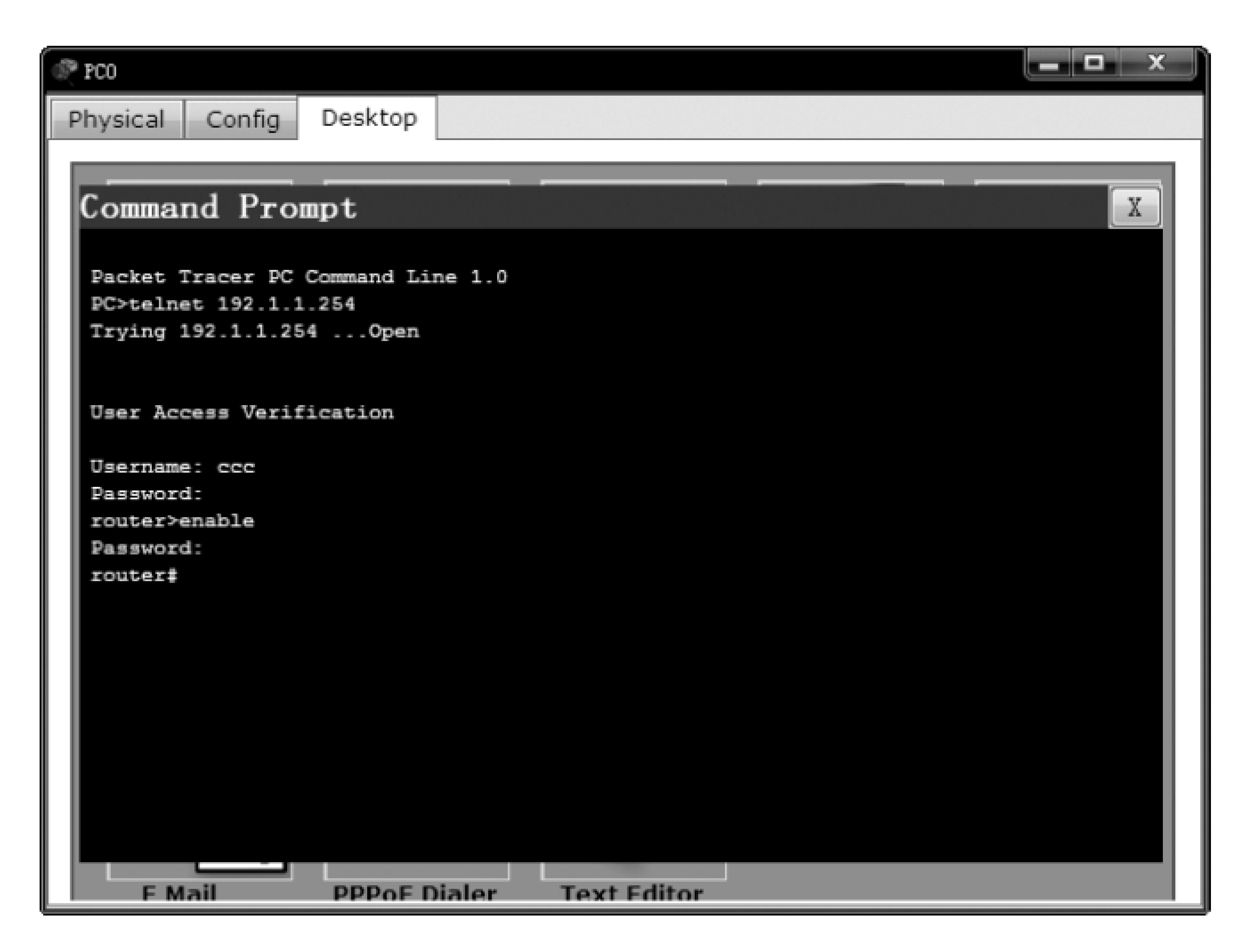


图 11.18 Telnet 登录 Router0 界面

4. 命令行配置过程

(1) Switch0 命令行配置过程

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.1.1.2 255.255.255.0
                                        (选择 VLAN 1 IP 接口地址作为交换机的管理地址)
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.1.1.254
```

```
                                                            (Router0 连接 Switch0 中 VLAN 1 接口的 IP 地址)
Switch(config)#enable password asdf                         (配置 enable 口令,使远程登录用户具有最高优先级)
Switch(config)#line vty 0 15
Switch(config-line)#password abc                            (通过口令验证远程登录用户身份)
Switch(config-line)#exit
```

(2) Switch1 命令行配置过程

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.1.2.2 255.255.255.0
                                                            (选择 VLAN 1 IP 接口地址作为交换机的管理地址)
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.1.2.254
                                                            (Router0 连接 Switch1 中 VLAN 1 接口的 IP 地址)
Switch(config)#enable password asdf
Switch(config)#username aaa password bbb                    (创建名为 aaa,口令为 bbb 的本地用户)
Switch(config)#line vty 0 15
Switch(config-line)#login local                             (通过本地用户信息验证远程登录用户身份)
Switch(config-line)#exit
```

(3) Router0 命令行配置过程

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#exit
Router(config)#aaa new-model                                (启动鉴别功能)
Router(config)#aaa authentication login a1 group radius
               (创建名为 a1 的远程登录鉴别机制,该机制通过 RADIUS 服务器鉴别远程登录用户身份)
Router(config)#hostname router                              (指定路由器的主机名为 router)
router(config)#enable password asdf
router(config)#radius-server host 192.1.2.1
                                                            (指定 RADIUS 服务器的 IP 地址是 192.1.2.1)
router(config)#radius-server key 1234
                                                (指定与 RADIUS 服务器交换数据时使用的密钥是 1234)
router(config)#line vty 0 15
router(config-line)#login authentication a1
                                                            (采用名为 a1 的鉴别机制鉴别远程登录用户身份)
```

```
router(config-line)#exit
```

11.3.3　SNMP 管理网络设备实验

1. 实验内容

(1) 完成网络设备 SNMP 配置。

(2) 确定被管对象的对象标识符。

(3) 查询被管对象的值。

(4) 设置被管对象的值。

(5) 验证被管对象值的查询和设置过程。

2. 网络结构

网络结构如图 11.19 所示。该实验是在 11.3.2 节 Telnet 方式配置网络设备实验的基础上进行，增加交换机连接的终端只是为了方便查询和设置交换机端口状态。Packet Tracer 有关网络设备 SNMP 配置比较简单，只有一条用于配置具有只读权限或读写权限的共同体的命令。

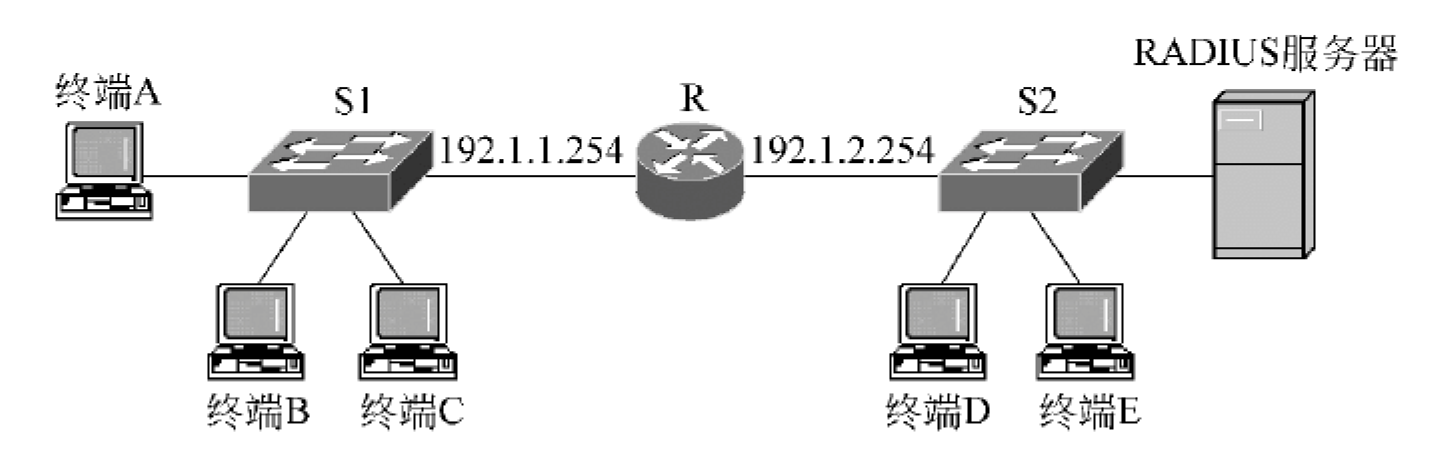


图 11.19　SNMP 网络管理系统

3. 实验步骤

(1) 启动 Packet Tracer，打开完成 11.3.2 节 Telnet 方式配置网络设备实验时存储的 PKT 文件，添加 PC1～PC4，生成图 11.20 所示的逻辑工作区界面。为 PC1～PC4 配置 IP 地址、子网掩码和默认网关地址。

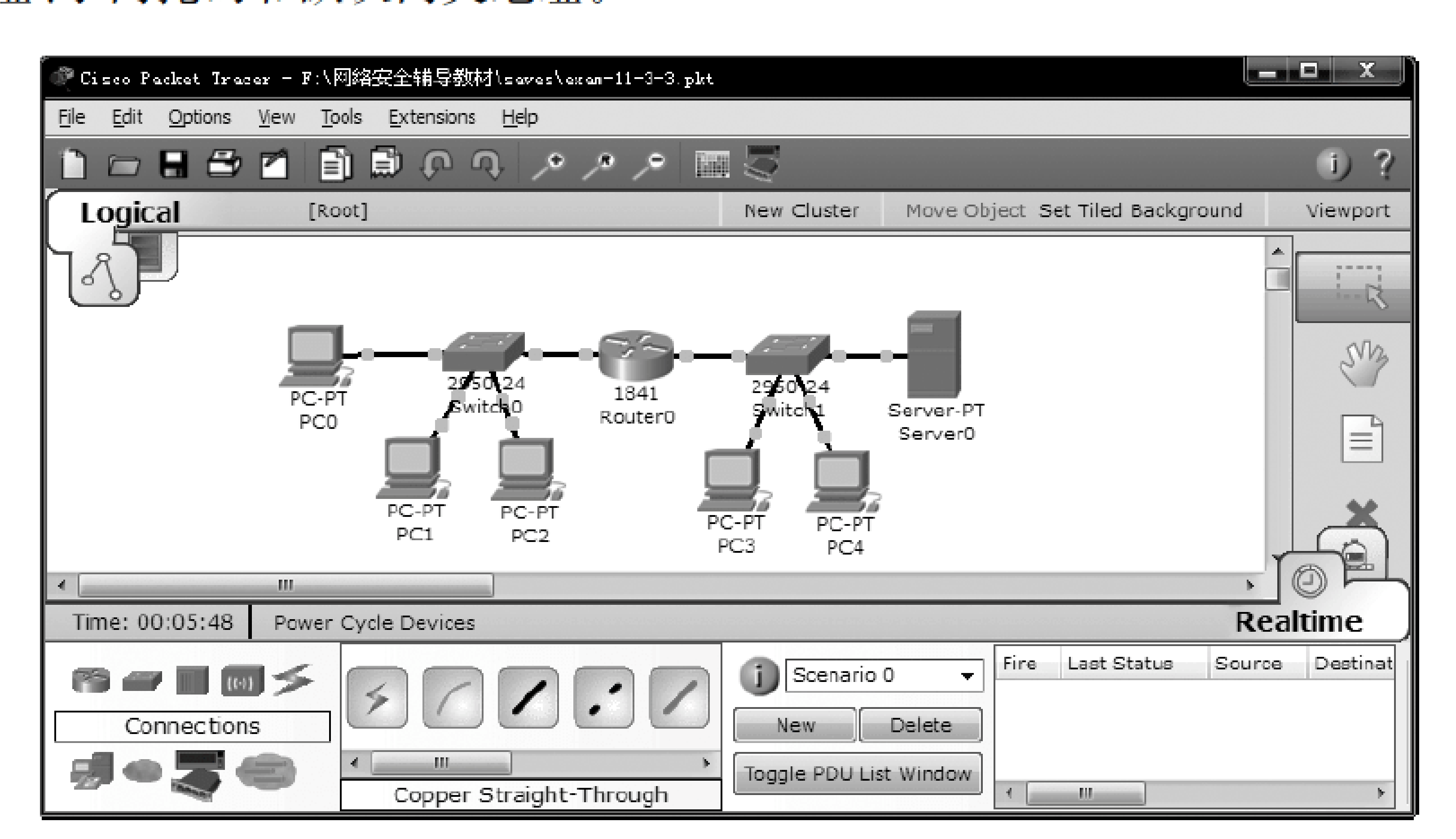


图 11.20　放置和连接设备后的逻辑工作区界面

(2) 对于各个网络设备,在全局配置模式下通过命令"snmp-server community asdf rw"启动 SNMP 管理网络设备功能,同时用公共体 asdf 作为读写 MIB 的通行证。

(3) 启动 PC0 桌面下的 MIB Browser 程序,出现图 11.21 所示界面,单击 Advanced 按钮,出现图 11.22 所示的 SNMP 配置界面,输入被管网络设备的 IP 地址,只读权限的公共体或读写权限的公共体,这里输入路由器 Router0 其中一个接口的 IP 地址 192.1.1.254 和读写权限公共体 asdf。



图 11.21　PC0 MIB Browser 界面

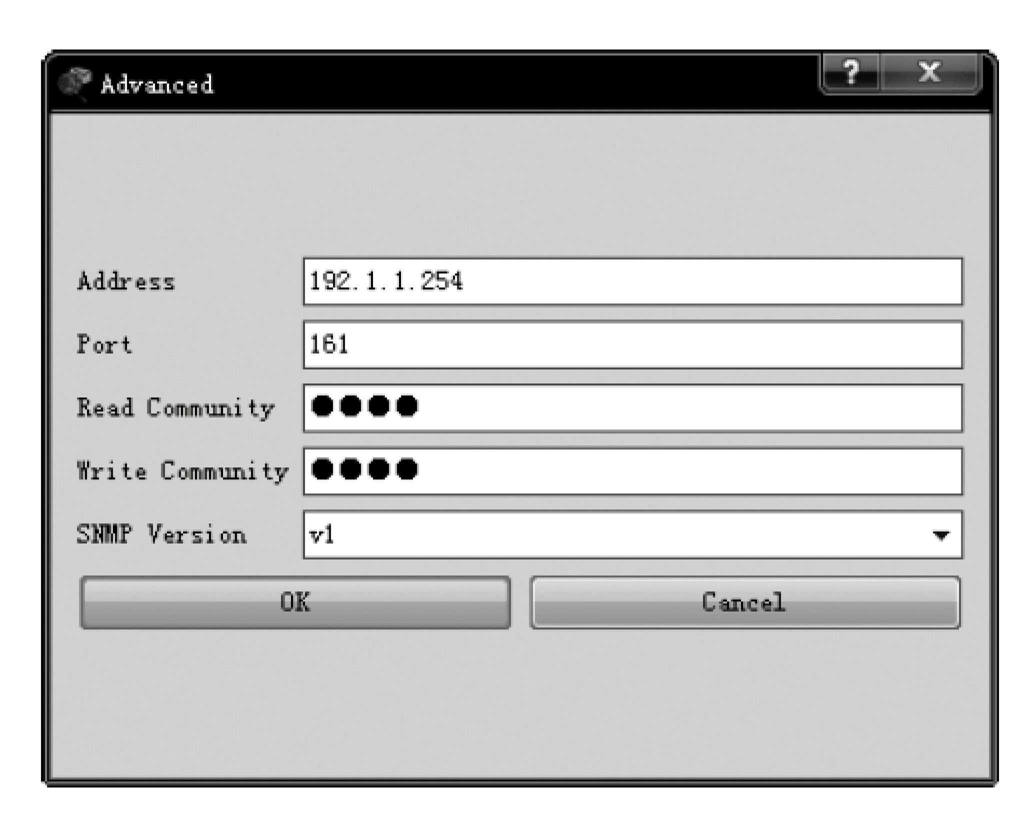


图 11.22　设置 SNMP 管理 Router0 界面

(4) 查询路由器接口 MAC 地址,在 SNMP MIBS 栏中展开被管对象节点,确定被管对象 iso.org.dod.internet.mgmt.mib-2.interface.ifTable.ifEntry.ifPhysAddress。在 Operations(操作)下拉列表中选中 Get 命令,单击 GO 按钮,Result Table(结果表)栏中出现路由器接口的 MAC 地址,操作结果如图 11.23 所示。Router0 总共有三个接口:两

个物理接口 FastEthernet0/0 和 FastEthernet0/1，一个 VLAN 1 接口。其中两个物理接口的 MAC 地址可以通过路由器接口配置界面获得，图 11.24 是接口 FastEthernet0/0 的配置界面，其 MAC 地址与通过 SNMP 查询到的其中一个接口的 MAC 地址相同。

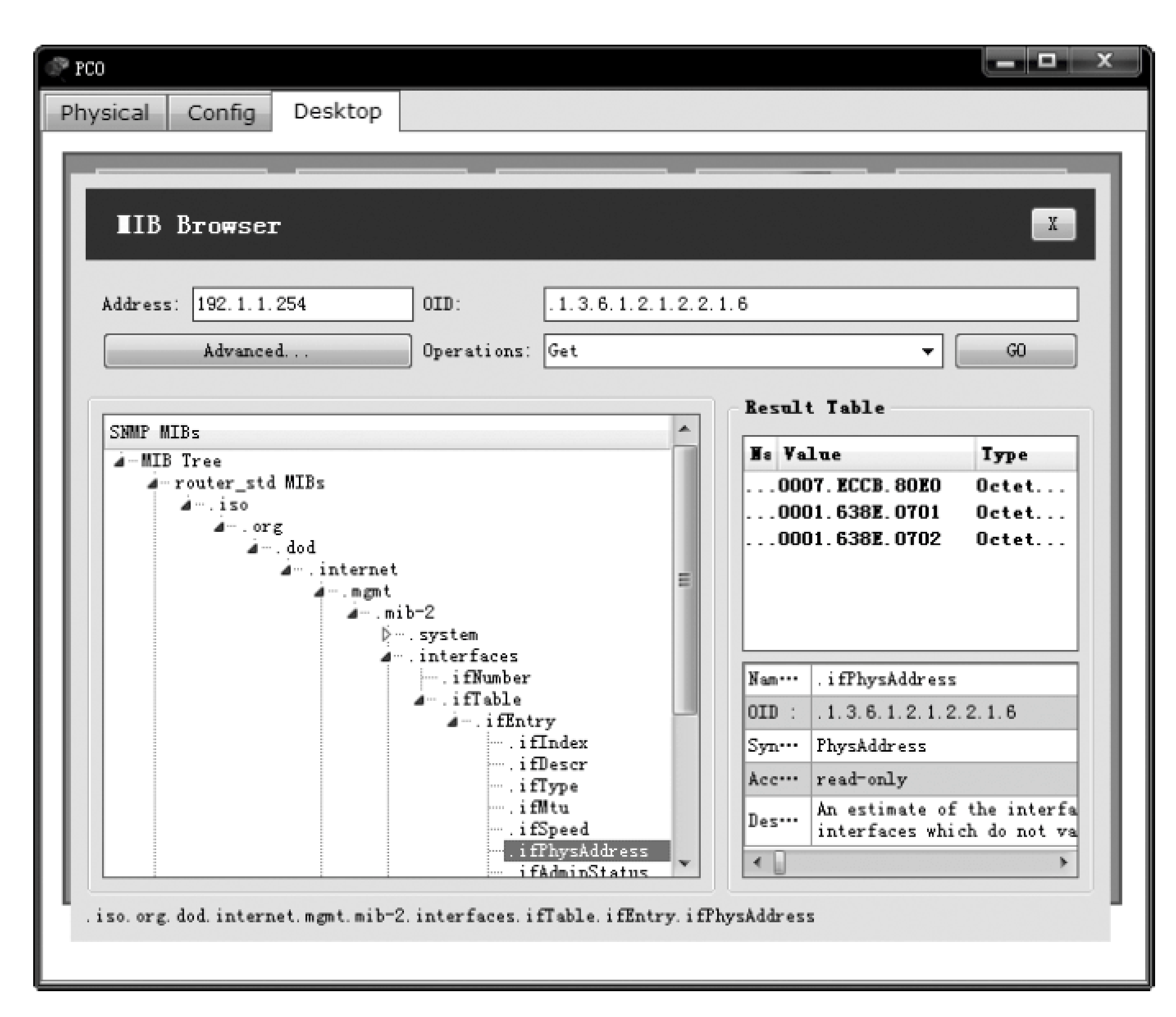


图 11.23 PC0 查询 Router0 接口 MAC 地址界面

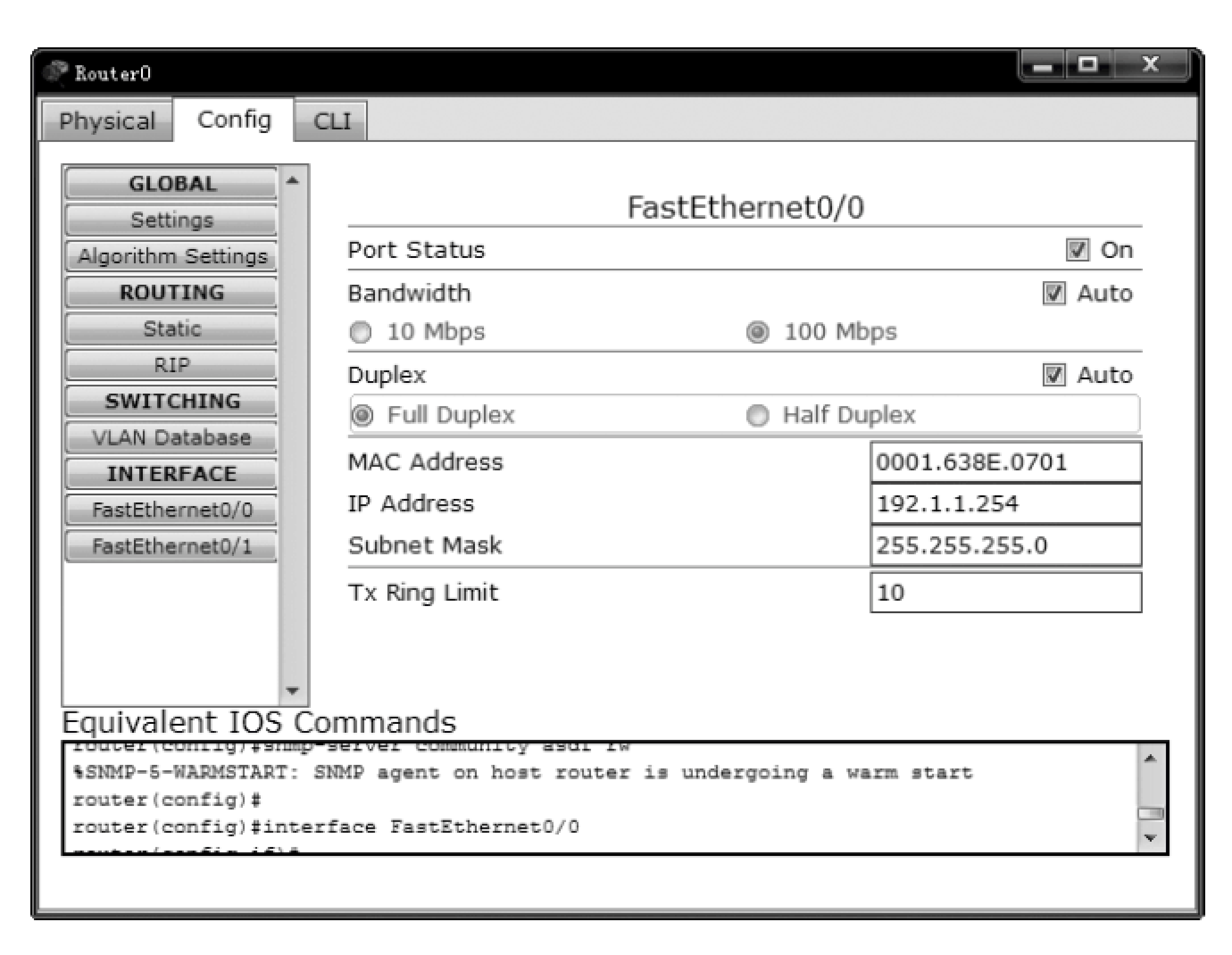


图 11.24 Router0 接口 FastEthernet0/0 的 MAC 地址

(5) 完成图 11.25 所示管理 Switch1 的 SNMP 配置。查询 Switch1 的端口状态，在 SNMP MIBS 栏中展开被管对象节点，确定被管对象 iso.org.dod.internet.mgmt.mib-2.interface.ifTable.ifEntry.ifAdminStatus。在 Operations 下拉列表中选中 Get 命令，单击 GO 按钮，Result Table 栏中出现 Switch1 所有端口的状态。Switch1 共有 25 个

端口：FastEthernet0/1～FastEthernet0/24，以及 VLAN 1 端口。目前处于 UP 状态的端口有 FastEthernet0/1 ～ FastEthernet0/4，以及 VLAN 1 端口。操作过程如图 11.26 所示。

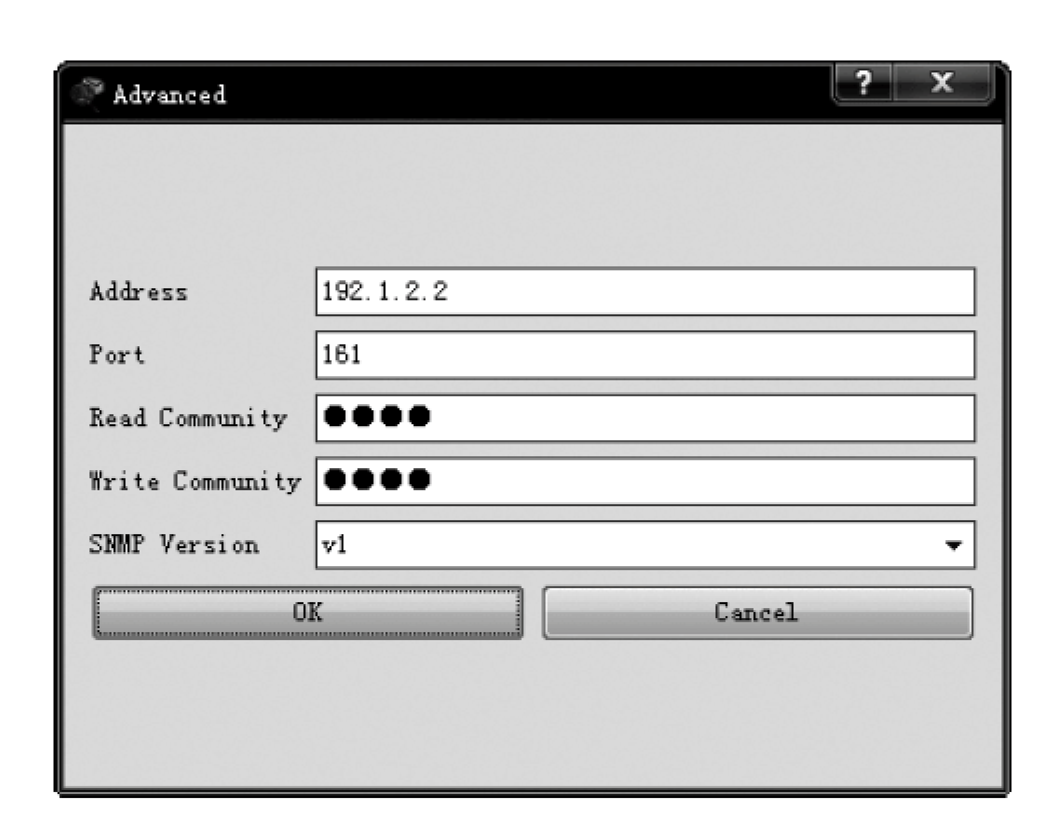


图 11.25　设置 SNMP 管理 Switch1 界面

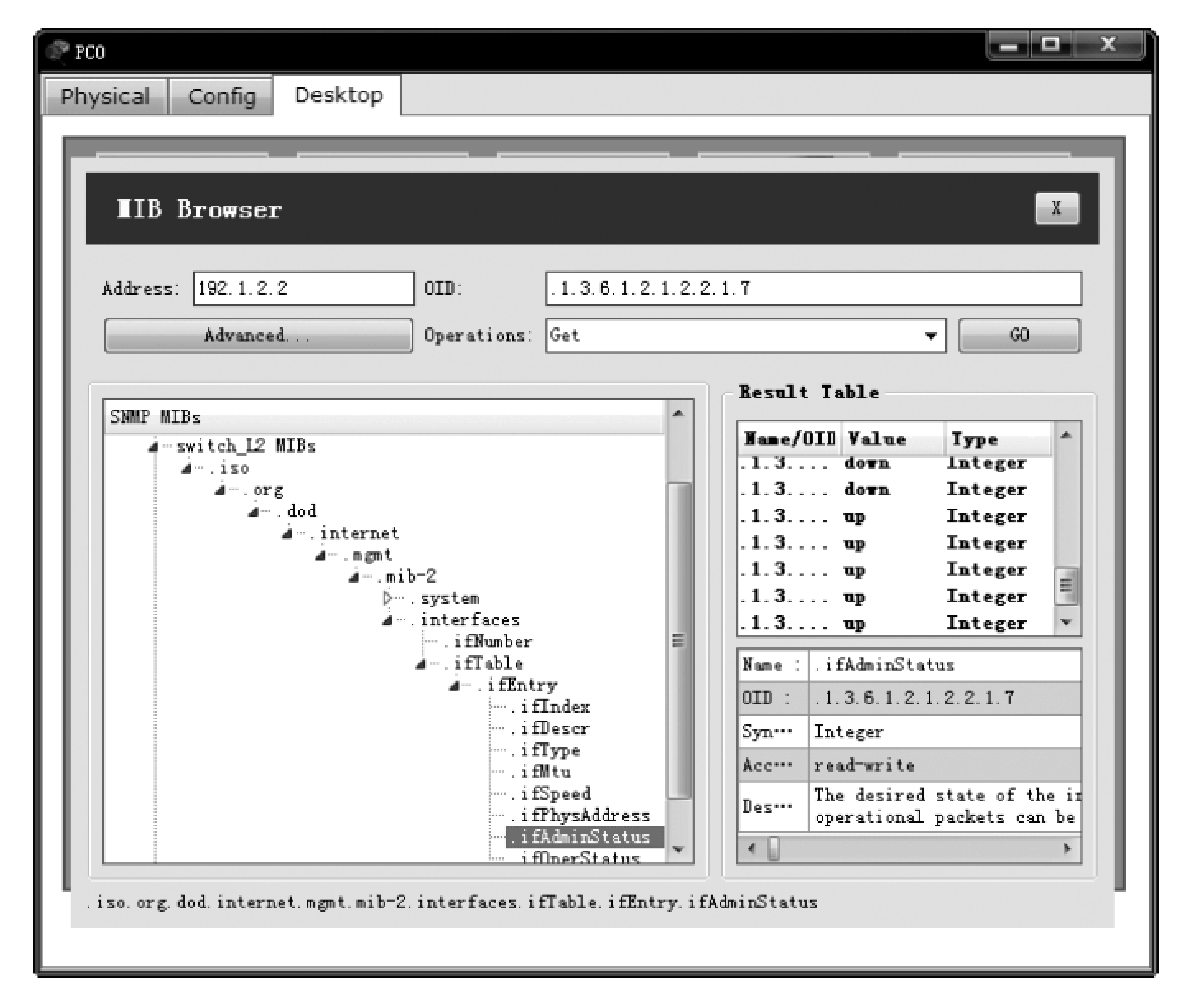


图 11.26　PC0 查询 Switch1 端口状态界面

(6) 为了设置 FastEthernet0/3 端口状态，或者在 OID 文本框中输入 FastEthernet0/3 端口对应的 OID，或者在 Result Table 中选中 FastEthernet0/3 端口对应的状态。在 Operations 下拉列表中选中 SET 命令，出现图 11.27 所示的被管对象类型和值配置界面，在 Data Type(数据类型)下拉列表中选中 Integer，在 Value(值)文本框中输入 down 状态对应的值“2”，单击 OK 按钮完成被管对象类型和值配置过程，单击 GO 按钮，完成 FastEthernet0/3 端口状态设置过程。图 11.28 是完成 FastEthernet0/3 端口状态设置过

程后 Result Table 栏中的内容。

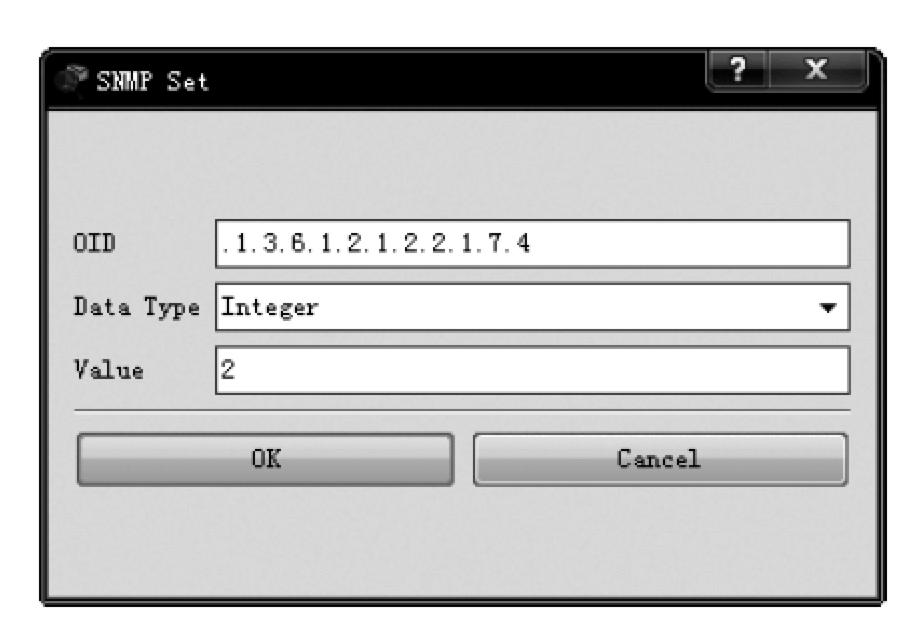


图 11.27 PC0 设置 Switch1 端口 FastEthernet0/3 状态界面

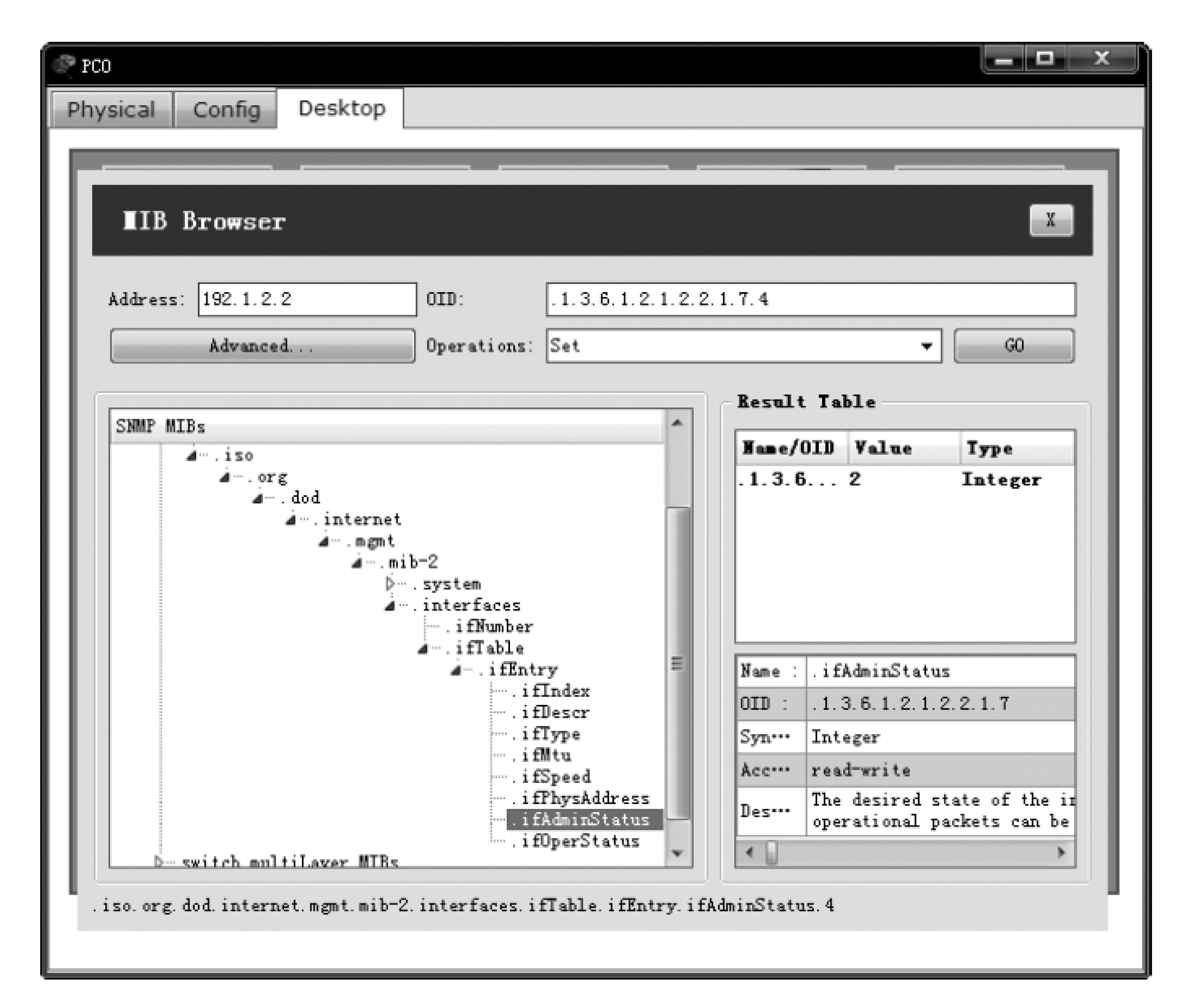


图 11.28 PC0 完成 Switch1 端口 FastEthernet0/3 状态设置后的界面

（7）在逻辑工作区界面发现 Switch1 连接 PC3 的端口 FastEthernet0/3 已经关闭，PC3 无法通过端口 FastEthernet0/3 发送和接收数据。

第12章 应用层安全协议

CHAPTER

12.1 知识要点

12.1.1 内部资源和公共资源

1. 资源性质

网络中的资源分布如图12.1所示，主要由内部资源和公共资源组成。公共资源连接在公共网络上，分配全球IP地址，对所有接入Internet的用户都是可见的。内部资源连接在内部网络中，分配本地IP地址，对外部用户是透明的。

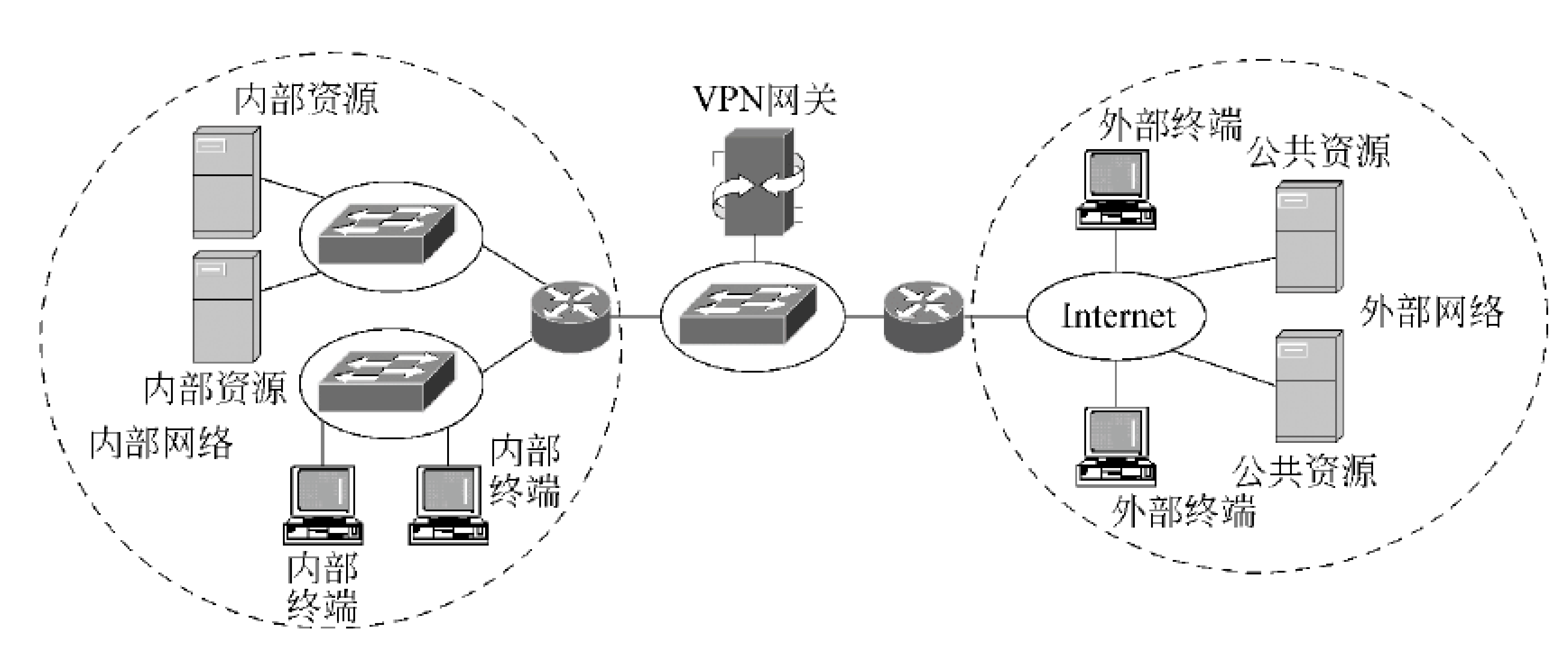


图12.1 资源分布结构

2. 访问控制的区别

(1) 内部资源访问控制

内部资源的访问控制机制如下：

- 通过防火墙技术对内部终端访问内部资源过程实施控制，只允许特定终端访问到内部资源；
- 通过入侵防御系统对入侵内部资源的行为进行监测和反制；
- 通过Kerberos访问控制技术对内部资源实施授权访问，限制每一个用户访问内部资源的权限；

- 通过 NAT 技术隐藏内部资源；
- 通过 VPN 网关对外部用户访问内部资源过程实施精细控制。

(2) 公共资源访问控制

- 允许所有终端访问公共资源；
- 由于提供公共服务，一般不会实施授权访问；
- 资源服务器自身实现访问控制和资源保护。

3. 公共资源的安全要求

公共资源由于提供公共服务，需要满足下述安全要求。

- 单向鉴别，需要鉴别公共资源提供者的身份，一般无需鉴别访问者的身份；
- 安全传输，访问公共资源需要经过公共网络传输数据，保证经过公共网络传输数据的保密性和完整性至关重要；
- 由于公共资源服务对象的广泛性，无法采用共享密钥身份鉴别机制，需要通过证书和数字签名验证公共资源提供者的身份；
- 实现安全传输的加密密钥和消息鉴别码(Message Authentication Code，MAC)密钥需要动态生成。

12.1.2 安全协议的适用性

1. 安全协议分类

安全协议分为两类：一类是在特定层实现上层 PDU 安全传输的协议，如 IP 安全(IP Sec)协议和传输层安全(Transport Layer Security，TLS)协议。前者实现传输层报文的安全传输，后者实现应用层报文的安全传输。另一类是为特定应用开发的安全协议，如 DNS 安全(DNS Sec)协议和安全电子交易(Secure Electronic Transaction，SET)协议。前者用于保证域名解析结果的准确性和完整性，后者用于实现网络购物和网络支付。

2. DNS Sec 的适用性

用户往往用完全合格域名标识服务器，在实际访问该服务器前，必须通过该完全合格域名得到对应服务器的 IP 地址，该过程就是域名解析过程，由域名系统(Domain Name System，DNS)实现。为了保证域名解析结果的准确性，要求做到：只允许合法的域名服务器参与域名解析过程，域名解析结果只能来自合法的域名服务器且传输过程中没有被篡改。这就需要对接收到的 DNS 响应报文进行如下处理：一是进行源端身份鉴别，以此确定该 DNS 响应报文是否由合法域名服务器发送。二是进行完整性检测，以此确定该 DNS 响应报文传输过程中是否被篡改。DNS Sec 通过数字签名技术实现了这一功能。

3. TLS 的适用性

TLS 被广泛用于公共资源访问过程，如访问公共的 Web 网站。对于这种客户端/服务器结构，一是需要单向鉴别，即客户需要鉴别服务器身份，防止黑客假冒公共资源提供者提供伪造的公共资源。二是客户端和服务器之间需要实现安全传输功能。三是由于客户端和服务器之间没有固定的关联，需要通过证书和数字签名，而不是共享密钥鉴别对方身份。由于 IP Sec 建立双向安全关联时需要实现双向身份鉴别，因此 IP Sec 并不适合用于公共资源访问过程。

4. SET 的适用性

SET 需要解决的是用户、商家和银行三方之间的身份鉴别和安全传输，重点在于既要绑定交易和支付，又要避免商家获得支付信息、银行获得交易信息，同时为了避免发生纠纷，必须保证所有发送消息的不可抵赖性。

12.2　例题解析

12.2.1　自测题

1. 选择题

(1) ________可以证明数据发送端、保障数据的完整性及防止重放攻击。

A. AH　　B. ESP　　C. TLS　　D. SET

(2) 下述________不是 DNS Sec 的功能。

A. 源端鉴别　　B. 完整性检测

C. 加密资源记录　　D. 域名与 IP 地址绑定关系验证

(3) 下述________与 DNS Sec 验证域名和 IP 地址绑定关系无关。

A. 增加表示域与公钥之间绑定关系的资源记录

B. 增加用于证明子域与公钥之间绑定关系的资源记录

C. 数字签名

D. 域名服务器之间用共享密钥鉴别对方身份

(4) 下述关于 TLS 的描述________是错误的。

A. TLS 可以实现双向身份鉴别

B. TLS 动态约定双方使用的安全参数

C. TLS 只能用于 HTTP

D. TLS 握手协议是一种比较通用的双向鉴别协议

(5) 下述关于 HTTPS 的描述________是错误的。

A. 客户通过 TLS 鉴别服务器身份

B. 客户和服务器通过 TLS 动态约定双方使用的安全参数

C. 处理后的 HTTP PDU 作为 TLS 记录协议的净荷

D. 记录协议的类型字段区分不同的应用层协议

(6) 下述关于 SET 的描述________是错误的。

A. 客户、商家和支付网关用证书和数字签名证明身份

B. 用数字签名保证发送消息的不可抵赖性

C. 用数字信封解决对称密钥的分发问题

D. 商家必须保证对用户信用卡信息保密

(7) 下述关于 SET 的描述________是错误的。

A. 用双重签名绑定支付信息和订货信息

B. 支付信息对商家是保密的

C. 银行无需知道订货信息

D. 用户直接向银行发送支付信息

(8) 下述关于 PGP 的描述________是错误的。

A. 发送端和接收端需事先获得对方公钥

B. 用数字信封传输对称密钥

C. 用数字签名实现源端鉴别和完整性检测

D. 用 TLS 实现双向身份鉴别

(9) 下述关于 S/MIME 的描述________是错误的。

A. 发送端和接收端需事先获得对方公钥

B. 用数字信封传输对称密钥

C. 用数字签名实现源端鉴别和完整性检测

D. 需用第三方软件实现加密和数字签名

(10) 下述________与应用层安全无关。

A. 实现双向身份鉴别

B. 安全传输消息

C. 数字签名实现发送消息的不可抵赖性

D. 防止经过网络传输的消息被嗅探和截获

2. 填空题

(1) ________用于两个终端间安全传输________,________用于两个进程间安全传输________,________对于中间经过的路由器是透明的。

(2) HTTPS 中 TLS 的作用是________和________,实现________需要 TLS 握手协议约定________、________、________、________和________等安全参数。

(3) PGP 的作用是________、________和________,其中通过数字签名实现________和________,采用________加密算法加密数据,通过________实现对称密钥分发,________其实是用________加密________后生成的密文。

(4) SET 的作用是实现________、________和________三方之间的________、________、________和________安全功能。通过________绑定交易和支付。

(5) 应用层安全功能主要包括________和________,一般通过证书和数字签名实现________,实现________需要双方动态约定________、________、________和________等安全参数。目前________在网络层提供________和________。________在传输层提供________和________。

3. 名词解释

____ PGP　　　　____ S/MIME

____应用层安全协议　　　　____ HTTPS

____ SET　　　　____ DNS Sec

(a) 一种对两端应用层实体进行身份鉴别,并保证两端应用层实体为实现某个应用所需要的信息交换过程安全进行的协议。

(b) 一种利用 TLS 双向身份鉴别功能和安全传输功能实现 Web 客户端和服务器之

间信息交换过程安全进行的协议。

(c) 一种广泛应用的数字签名和加密软件,用于实现数据的源端鉴别和安全传输、存储。

(d) 为实现邮件源端鉴别和安全传输,在 MIME 邮件格式基础上增加了数字签名和密文内容类型后的邮件格式。

(e) 一个为了在因特网上进行在线交易而设立的,开放的、以电子货币为基础的电子支付系统规范。

(f) 一种 DNS 安全扩展标准,增加了通过数字签名对 DNS 响应报文进行源端鉴别和完整性检测的功能。

4. 判断题

(1) 应用层安全的主要目的是实现双向身份鉴别和两端实体之间的安全传输。

(2) TLS 客户端身份鉴别功能是可选的。

(3) PGP 是一个具有数字签名和加密功能的软件,可以用于实现邮件的安全传输。

(4) HTTPS 没有使客户端和服务器之间交换的报文具有不可抵赖性。

(5) DNS Sec 一是增加了通过数字签名对 DNS 响应报文进行源端鉴别和完整性检测的功能,二是增加了用于证明域和公钥之间绑定关系的资源记录。

(6) TLS 记录协议具有区分不同应用层报文的字段。

(7) 应用层安全协议能解决一切网络安全问题。

(8) 网络安全就是指主机系统安全和访问安全。

(9) 可以用 HTTPS 取代 SET。

(10) SET 的主要作用是实现安全的网络购物和电子支付。

(11) 各方交换的 SET 消息具有不可抵赖性。

(12) 证书和数字签名是一种最广泛的身份鉴别机制。

12.2.2　自测题答案

1. 选择题答案

(1) A,AH 是唯一对源 IP 地址进行完整性检测的安全协议。

(2) C,DNS Sec 不对资源记录加密。

(3) D,DNS Sec 通过数字签名验证 DNS 响应报文的源端和完整性。

(4) C,TLS 作为传输层安全协议,可以作用于多种应用层协议。

(5) D,通过 TCP 的端口号来区分使用 TLS 的应用层协议。

(6) D,SET 不会使商家获得用户的信用卡信息。

(7) D,由商家完成用户支付能力验证,向银行发送支付请求。

(8) D,PGP 不使用 TLS。

(9) D,支持 S/MIME 的客户代理直接实现加密和数字签名。

(10) D,这一项不是两端应用层实体所能控制的。

2. 填空题答案

(1) IP Sec,传输层报文,TLS,应用层报文,TLS。

(2) 实现客户对服务器的身份鉴别,客户端和服务器之间安全传输 HTTP 报文,客户端和服务器之间安全传输 HTTP 报文,压缩算法,加密算法,MAC 算法,加密密钥,MAC 密钥。

(3) 源端鉴别,加密,完整性检测,源端鉴别,完整性检测,对称密钥,数字信封,数字信封,接收端公钥,对称密钥。

(4) 用户,商家,支付网关,源端鉴别,完整性检测,加密,不可抵赖发送过的消息,双重签名。

(5) 双向身份鉴别,两端实体之间的安全传输,身份鉴别,两端实体之间的安全传输,加密算法,MAC 算法,加密密钥,MAC 密钥,IP Sec,发送端和接收端之间的双向身份鉴别,发送端和接收端之间传输层报文的安全传输,TLS,两端实体之间的双向身份鉴别,两端实体之间应用层报文的安全传输。

3. 名词解释答案

c PGP	d S/MIME
a 应用层安全协议	b HTTPS
e SET	f DNS Sec

4. 判断题答案

(1) 对,这是两端应用层实体提供的安全功能。

(2) 对,TLS 只有对服务器端的身份鉴别是必须的。

(3) 对,PGP 是一个广泛使用的具有数字签名和加密功能的软件。

(4) 对,TLS 没有对净荷附加数字签名。

(5) 对,DNS Sec 因此可以通过数字签名实现源端鉴别和完整性检测。

(6) 错,通过 TCP 的端口号来区分使用 TLS 的应用层协议。

(7) 错,网络资源的可用性不是通过应用层安全协议可以实现的。

(8) 错,还应该包括网络和网络资源的可用性,如防御拒绝服务攻击。

(9) 错,SET 提供的安全交易和安全支付功能不是 TLS 能够实现的。

(10) 对,SET 是为了在因特网上进行在线交易而设立的,开放的、以电子货币为基础的电子支付系统规范。

(11) 对,无法抵赖发送过的消息是实现安全交易和安全支付的基础。

(12) 对,任何实体只要提供证明某个标识符与某个公钥之间绑定关系的证书,且能够通过数字签名证明自己拥有该公钥对应的私钥,就能够证明自己就是该标识符宣示的实体。

12.2.3 简答题解析

1. 简述应用层安全的功能及在网络安全中的地位。

回答:网络安全需要保证网络通信畅通,主机系统健壮,两个应用层实体之间的信息交换过程能够准确和安全地进行。应用层安全实现的两个应用层实体之间双向身份鉴别和安全数据传输功能只是保证了两个应用层实体之间的信息交换过程能够准确和安全地进行,无法保证网络通信畅通和主机系统健壮。

2. 结合 DNS Sec，给出解决 Host 劫持攻击的方法。

回答： Host 文件中的缓存项给出域名和 IP 地址之间的绑定关系，如果主机需要解析的域名包含在某项有效的缓存项中，主机无需通过域名系统解析该域名，而是直接用该缓存项中的 IP 地址作为该域名的解析结果。黑客一旦篡改了 Host 文件中某项缓存项中的 IP 地址，则主机通过 Host 文件解析到的结果就是黑客伪造的 IP 地址，这就是黑客的 Host 劫持攻击，可以将用户对某个用完全合格域名标识的服务器的访问变为对黑客设计的主机系统的访问。

为了解决黑客的 Host 劫持攻击，对每一项给出域名和 IP 地址之间绑定关系的缓存项进行数字签名，同时通过证明链指定用于验证该数字签名的公钥。

第13章 试卷和答案

CHAPTER

13.1 试 卷 一

13.1.1 试卷

一、选择题(本大题共 20 小题,每小题 1 分,共 20 分)

(1) 下述________不属于引发网络安全问题的原因。

A. 网络原旨是方便通信

B. 大量商务活动在网上展开

C. 网络信息资源已经成为重要的战略资源

D. 网络安全设备发展迅速

(2) 下述________无法破坏网络的可用性。

A. 病毒　　B. 拒绝服务攻击

C. 非法访问　　D. 线缆遭受破坏

(3) 下述________和诱骗用户登录伪造的著名网站无关。

A. 篡改 DNS 服务器的资源记录

B. 伪造 DNS 服务器

C. 配置主机系统网络信息方式

D. 著名网站的物理安保措施

(4) 下述________表示黑客们编写的旨在破坏其他主机系统的代码集合。

A. 恶意代码　　B. 病毒　　C. 木马　　D. 蠕虫

(5) 下述________表示黑客们编写的旨在非法访问其他主机系统中信息资源的代码。

A. 恶意代码　　B. 病毒　　C. 木马　　D. 蠕虫

(6) 下述________不是阻止病毒实施破坏操作的措施。

A. 安装主机入侵防御系统

B. 监控内部网络终端发起建立的 TCP 连接

C. 禁止读写移动存储媒介

D. 对主机系统中重要文件加密

(7) 网络入侵防御系统对下述________病毒传播方式不起作用。
A. 利用主机系统漏洞自动传播病毒
B. 通过邮件传播病毒
C. 通过 Web 页面传播病毒
D. 通过实用程序传播病毒

(8) 下述________是解决主机系统漏洞的较好办法。
A. 消灭主机系统漏洞
B. 不让黑客知道已经发现的主机系统漏洞
C. 网络隔绝黑客扫描主机系统的途径
D. 将存在漏洞的主机系统和网络断开

(9) 缓冲器溢出的最大危害是________。
A. 使系统崩溃　B. 使系统运行出错
C. 管理员权限下运行黑客程序　D. 侵占其他用户内存

(10) SYN 泛洪攻击利用________。
A. 操作系统漏洞　B. 通信协议缺陷
C. 缓冲区溢出　D. 用户警惕性不够

(11) 现代密码体制用下述________保证密文安全性。
A. 保密加密算法　B. 保密解密算法
C. 保密加密密钥　D. 保密解密密钥

(12) 好的加密算法只能采用下述________方法破译密文。
A. 穷举　B. 数学分析　C. 明文和密文对照　D. 分析密文规律

(13) 下述________不是 RSA 加密算法的特点。
A. 公钥和私钥不同　B. 无法根据公钥推导出私钥
C. 密文和明文等长　D. 可靠性基于大数因子分解困难的事实

(14) 下述________算法属于对称密钥算法。
A. RSA　B. MD5
C. Diffie-Hellman 密钥交换算法　D. 流密码

(15) 下述________算法属于不对称密钥算法。
A. RSA　B. MD5　C. DES　D. AES

(16) 对于 PPP,下面________描述是错误的。
A. 基于点对点信道的链路层协议
B. PSTN 作为接入网络时的接入控制协议
C. 通过 PPP over X 技术实现 PPP 帧经过多种类型的分组交换路径的传输过程
D. 通用的链路层协议

(17) 用户终端通过拨号接入方式接入 Internet 需要 Modem 的原因是________。
A. 用户线只能传输模拟信号
B. 通过呼叫连接建立过程建立用户终端与接入控制设备之间的点对点信道
C. 接入控制设备需要通过 PPP 实现对用户终端的接入控制

D. A 和 B

(18) 图 13.1 是 NAT 的一个示例，根据图 13.1 中的信息，标号为①的箭头线所对应的方格内容应是 。

A. S=192.168.1.1:3105　D=202.113.64.2:8080
B. S=59.67.148.3:5234　D=202.113.64.2:8080
C. S=192.168.1.1:3105　D=59.67.148.3:5234
D. S=59.67.148.3:5234　D=192.168.1.1:3105

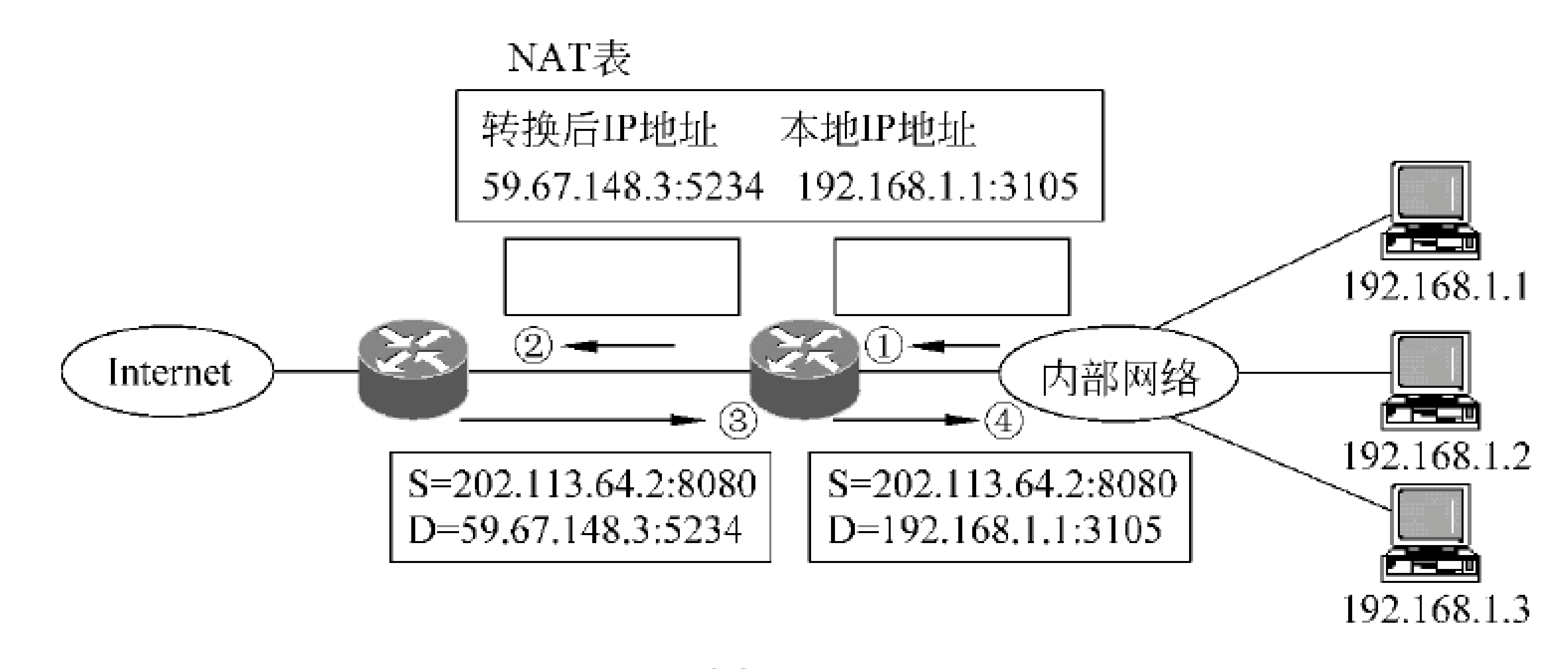


图 13.1

(19) 下述________是实现接入控制的前提。

A. 建立允许接入的授权用户的标识信息列表
B. 互连接入网络和 Internet 的路由器具有接入控制功能
C. 鉴别协议能够实现用户身份鉴别
D. 以上全是

(20) 对于具有 PPP 接入功能的设备，下述________描述是最贴切的。

A. 必须是路由器　B. 必须是交换机
C. 可以是交换机　D. 没有交换和路由功能的设备

二、填空题(本大题共 20 空，每空 1 分，共 20 分)

(1) 信息安全目标是保证信息的________、________、________、________和________。

(2) 计算机网络面临的主要威胁有________和________。

(3) 目前常见的恶意代码包括________、________、________和________。

(4) 目前常见的基于主机系统的防病毒措施包括________、________和________，其中________的作用是发现正在运行的病毒和被病毒感染的文件，________的作用是关闭病毒传播到主机系统的通路，________的作用是监控病毒感染主机系统过程。

(5) 对称密钥算法的主要缺点包括________、________和________。

三、简答题(本大题共 5 小题，每题 4 分，共 20 分)

1. 简述防止黑客远程入侵主机系统机制。
2. 简述阻止病毒传播和危害发生的措施。
3. 简述恶意代码长期存在的理由。
4. 简述安全加密算法的特点。

5. 简述信息安全的基础是加密算法的理由。

四、判断题(本大题共 10 小题,每小题 1 分,共 10 分)

(1) 只要目的地址正确,分组不会错误地传输给其他终端。

(2) 只要安装杀毒软件,定时更新病毒特征库,就不可能感染病毒。

(3) 操作系统和应用程序漏洞是蠕虫入侵的主要渠道。

(4) 在无数漏洞中,缓冲器溢出漏洞是危害较大的一种漏洞。

(5) 缓冲器溢出漏洞是蠕虫得以快速传播的主因。

(6) 加密算法在网络安全中的作用仅仅是加密传输的数据。

(7) 不存在摘要相同的两个不同报文。

(8) 分组密码的数据段长度和加密运算的复杂性有关。

(9) 身份鉴别和源端鉴别是完全相同的。

(10) 数字签名可以实现源端鉴别。

五、综合题(本大题共 3 小题,每小题 10 分,共 30 分)

1. 网络结构如图 13.2 所示。终端通过 DHCP 自动配置网络信息,并以域名 www.baidu.com 访问 IP 地址为 192.1.3.7 的 Web 服务器。要求:

① 给出 DHCP 服务器和 DNS 服务器中与实现域名解析相关的配置。

② 如果通过图中伪造的 DHCP 服务器和伪造的 DNS 服务器错误地将域名 www.baidu.com 与 IP 地址 192.1.2.3 绑定,给出伪造的 DHCP 服务器和伪造的 DNS 服务器中与实现错误的域名解析相关的配置。

③ 给出防止图中伪造的 DHCP 服务器和伪造的 DNS 服务器实现错误的域名解析的方法。

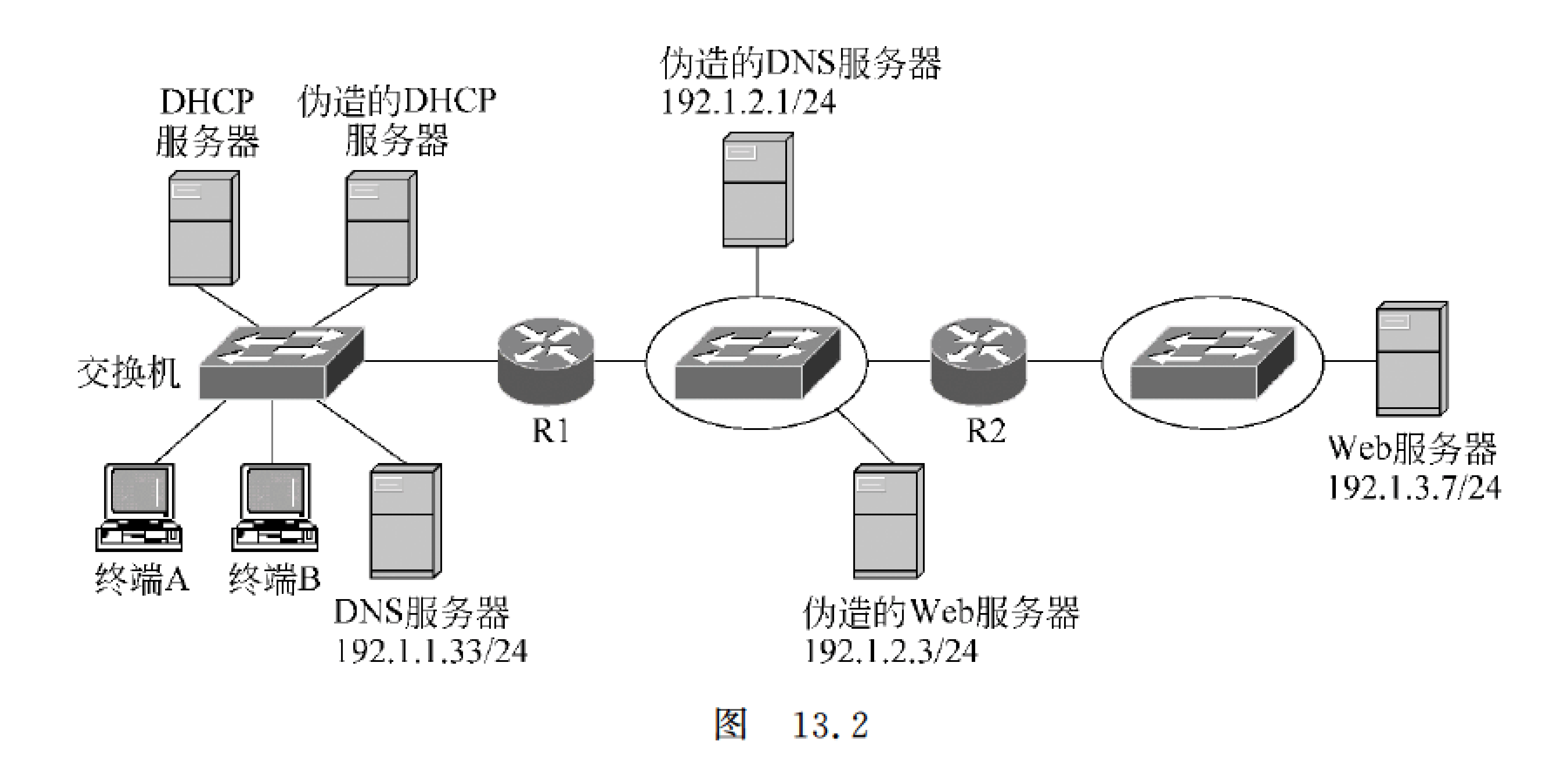


图 13.2

2. 网络结构如图 13.3 所示。要求禁止终端 A、终端 B 和终端 C 之间相互通信,但允许这三个终端和其他终端相互通信,同时也允许其他终端之间相互通信,请给出需要配置的无状态分组过滤器,并说明作用接口和方向。

3. 网络结构如图 13.4 所示。回答以下问题。

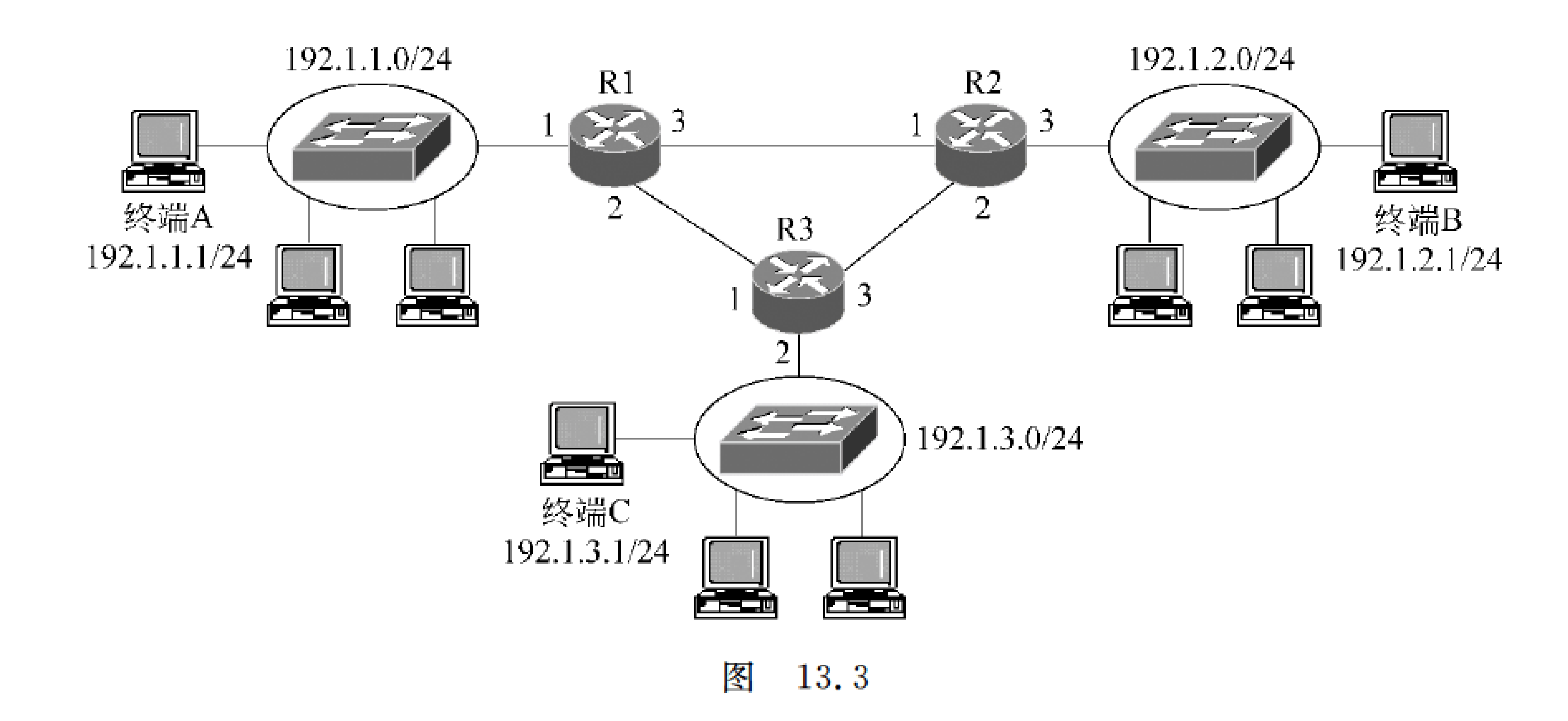


图　13.3

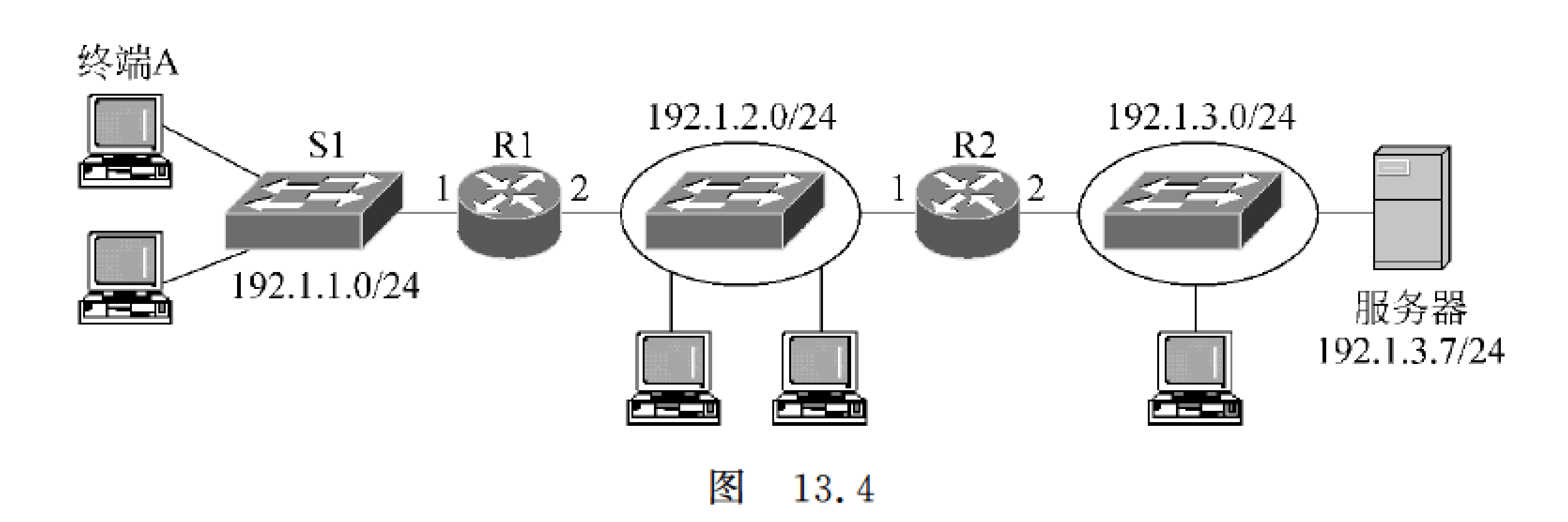


图　13.4

① 如果终端 A 想要通过 Smurf 攻击瘫痪服务器，给出终端 A 发送的 ICMP ECHO 请求报文的源和目的 IP 地址。

② 如果要求网络能够阻止终端 A 发起对服务器的 Smurf 攻击，给出在交换机 S1、路由器 R1 和 R2 上采取的措施。

13.1.2　答案

一、选择题答案

1. D　2. C　3. D　4. A　5. C　6. C　7. D　8. C　9. C
10. B　11. D　12. A　13. C　14. D　15. A　16. D　17. D　18. A
19. D　20. A

二、填空题答案

1. 保密性，完整性，可用性，不可抵赖性，可控制性。

2. 非法访问，拒绝服务攻击。

3. 狭义病毒，蠕虫，木马，逻辑炸弹。

4. 查杀病毒软件，个人防火墙，主机入侵防御系统，查杀病毒软件，个人防火墙，主机入侵防御系统。

5. 密钥分发困难，多对多通信持有的密钥数量大，数据保密性差。

三、简答题答案

1. **回答**：一是主机系统及时通过补丁软件消除漏洞；二是主机系统通过授权和身份

鉴别对信息资源访问过程进行监控；三是通过接入控制机制禁止非授权用户使用的终端接入网络；四是通过防火墙和入侵防御系统禁止与实施漏洞扫描和利用漏洞实施攻击相关的信息到达主机系统。

2. **回答**：这些措施分为基于主机系统的措施和基于网络的措施，基于主机系统的措施有及时运行补丁软件，安装查杀病毒软件、主机入侵防御系统和个人防火墙等。基于网络的措施有在网络边界设置控制网络间信息交换过程的防火墙，在关键链路设置严格监控流经该段链路的信息流的网络入侵防御系统，采用隐藏内部网络的 NAT 技术和限制疑似与病毒传播和拒绝服务攻击有关的信息流的流量的流量管制技术。

3. **回答**：导致恶意代码存在的主要原因是主机系统的漏洞，包括操作系统漏洞和应用程序漏洞。在未来较长一段时间内，不可能编写出没有安全漏洞的操作系统和应用程序，因此肯定会产生针对各种漏洞的恶意代码。网络是传播恶意代码的主要通道，网络安全技术无法完全阻隔病毒传播通路，也无法完全阻止黑客通过网络扫描到存在漏洞的主机系统，并通过网络将针对该漏洞的恶意代码上传到该主机系统并激活。

4. **回答**：一是加密运算必须足够复杂，除了通过穷举法破译密文外，没有其他更有效的破译密文的方法；二是密钥长度必须足够长，以此保证使用普通计算机破译密文时，用穷举法破译密文所需的时间超出密文的有效期，使用高性能计算机破译密文时，破译密文付出的代价超出密文信息价值；三是经过广泛试验，证明无法通过网格计算以较小成本用穷举法破译密文。

5. **回答**：一是加密算法是保证信息存储和传输过程中保密性的基础；二是加密算法和报文摘要算法是实现信息存储和传输过程中完整性检测的基础；三是加密算法是实现网络环境中身份鉴别、源端鉴别和数字签名的基础，而这些功能是许多网络应用的实现基础。

四、判断题答案

1. 错 2. 错 3. 对 4. 对 5. 对 6. 错 7. 错 8. 对 9. 错 10. 对

五、综合题答案

1. **回答**：① DHCP 服务器中必须给出域名服务器的 IP 地址 192.1.1.33。域名服务器中必须给出用于绑定域名 www.baidu.com 和 IP 地址 192.1.3.7 的 A 类型资源记录。

② 伪造的 DHCP 服务器中必须给出伪造的域名服务器的 IP 地址 192.1.2.1。伪造的域名服务器中必须给出用于绑定域名 www.baidu.com 和 IP 地址 192.1.2.3 的 A 类型资源记录。

③ 将连接 DHCP 服务器的交换机端口设置成信任端口，且交换机只转发通过信任端口接收到的 DHCP 响应报文。这样，所有连接在非信任端口的伪造的 DHCP 服务器发送的响应报文都被交换机丢弃。另外，也可以采用应用层安全协议 DNS Sec。

2. **回答**：为了禁止终端 A 与终端 B 和 C 通信，路由器 R1 接口 1 丢弃终端 A 发送的、目的终端为终端 B 或终端 C 的 IP 分组，但允许其他 IP 分组正常转发。同样，为了禁止终端 B 与终端 A 和 C 通信，路由器 R2 接口 3 丢弃终端 B 发送的、目的终端为终端 A 或终端 C 的 IP 分组，允许其他 IP 分组正常转发。为了禁止终端 C 与终端 A 和 B 通信，

路由器 R3 接口 2 丢弃终端 C 发送的、目的终端为终端 A 或终端 B 的 IP 分组，允许其他 IP 分组正常转发。各个路由器接口具体配置的分组过滤器如表 13.1 所示。

表　13.1

协议	源 IP 地址	目的 IP 地址	动作
路由器 R1 接口 1 输入方向			
IP	192.1.1.1/32	192.1.2.1/32	丢弃
IP	192.1.1.1/32	192.1.3.1/32	丢弃
IP	any(0.0.0.0/0)	any(0.0.0.0/0)	正常转发
路由器 R2 接口 3 输入方向			
IP	192.1.2.1/32	192.1.1.1/32	丢弃
IP	192.1.2.1/32	192.1.3.1/32	丢弃
IP	any(0.0.0.0/0)	any(0.0.0.0/0)	正常转发
路由器 R3 接口 2 输入方向			
IP	192.1.3.1/32	192.1.1.1/32	丢弃
IP	192.1.3.1/32	192.1.2.1/32	丢弃
IP	any(0.0.0.0/0)	any(0.0.0.0/0)	正常转发

3. **回答**：① 终端 A 发送三种类型的 ICMP ECHO 请求报文：一是源 IP 地址为 192.1.3.7，目的 IP 地址为受限广播地址 255.255.255.255 的 ICMP ECHO 请求报文。二是源 IP 地址为 192.1.3.7，目的 IP 地址为直接广播地址 192.1.2.255 的 ICMP ECHO 请求报文。三是源 IP 地址为 192.1.3.7，目的 IP 地址为直接广播地址 192.1.3.255 的 ICMP ECHO 请求报文。

② 交换机 S1 各个端口和 IP 地址绑定，从某个端口接收到 IP 分组时，只有源 IP 地址与该端口绑定的 IP 地址相同的 IP 分组才被允许正常转发。路由器 R1 接口 1 输入方向设置分组过滤器，只允许源 IP 地址属于网络地址 192.1.1.0/24 的 IP 分组正常转发。路由器 R1 禁止目的地址为直接广播地址的 IP 分组正常转发。路由器 R2 接口 1 输入方向设置流量管制器，限制以服务器 IP 地址为目的地址的 ICMP ECHO 响应报文的流量。路由器 R2 开启单播反向路径验证功能。

13.2　试　卷　二

13.2.1　试卷

一、选择题(本大题共 20 小题，每小题 1 分，共 20 分)

(1) 下述________和黑客远程入侵主机系统无关。

A. 操作系统漏洞　　　　B. 应用程序漏洞

C. 黑客和主机系统之间信息传输路径　D. 主机系统的物理安保措施

(2) 下述________和信息截获攻击有关。

A. 操作系统漏洞　B. 应用程序漏洞

C. 配置主机系统网络信息方式　D. 主机系统的物理安保措施

(3) 加密和报文摘要算法一般不能阻止下述________攻击。

A. 信息嗅探攻击　B. 信息截获攻击

C. 篡改信息攻击　D. 重放攻击

(4) 下述________攻击和操作系统漏洞无关。

A. 非法登录主机系统

B. 向主机系统植入病毒

C. 缓冲器溢出

D. 消耗掉主机系统连接网络的链路的带宽

(5) 下述________表示黑客们编写的、嵌入在正常程序中、具有自我复制能力的一段代码。

A. 恶意代码　B. 病毒　C. 木马　D. 蠕虫

(6) 蠕虫能够自动传播到某个主机系统并自动激活的原因是________。

A. 主机系统存在漏洞

B. 主机系统下载程序

C. 主机系统收发邮件

D. 主机系统之间用移动媒介复制文件

(7) 下述________病毒检测机制是检测系统软件是否感染病毒的有效方法。

A. 基于特征的扫描技术　B. 基于线索的扫描技术

C. 基于完整性检测的扫描技术　D. 基于行为的检测技术

(8) 防火墙能有效阻止下述________病毒传播方式。

A. 利用主机系统漏洞自动传播病毒　B. 通过邮件传播病毒

C. 通过 Web 页面传播病毒　D. 通过实用程序传播病毒

(9) 下述________不是对主机系统实施的拒绝服务攻击。

A. Ping of Death　B. SYN 泛洪

C. Smurf　D. 穷举法猜测用户登录口令

(10) 下述________是蠕虫病毒传播的主因。

A. 缓冲区溢出漏洞

B. 从服务器下载文件

C. 收发电子邮件

D. 通过移动媒介在主机系统间复制文件

(11) 下述________不是以破坏信息保密性为目的的攻击行为。

A. 信息嗅探　B. 信息截获　C. 安装后门程序　D. DDoS

(12) 下述________攻击行为与主机系统漏洞无关。

A. Ping of Death　B. Land　C. 安装后门程序　D. Smurf

(13) 加密算法安全性受到下述________挑战。

A. 网格计算　　B. 高速计算机　　C. 人工分析　　D. 数学分析

(14) 安全的加密算法具有下述________特点。

A. 只能用穷举法破译密文　　B. 密钥长度足够

C. 经得起网格计算考验　　D. 以上全部

(15) 网络安全中,加密算法的用途包含下述________。

A. 加密信息　　B. 信息完整性检测

C. 用户身份鉴别　　D. 以上全部

(16) 下述________是用 RSA 生成数字签名的先决条件。

A. 公钥和私钥一一对应

B. 私钥只有签名者自己知道

C. 由权威机构证明公钥和签名者之间绑定

D. 以上全部

(17) 图 13.5 是 NAT 的一个示例,根据图 13.5 中的信息,标号为④的箭头线所对应的方格内容应是________。

A. S=135.2.1.1:80　　B. S=135.2.1.1:80
D=202.0.1.1:5001　　D=192.168.1.1:3342

C. S=135.2.1.1:5001　　D. S=192.168.1.1:3342
D=135.2.1.1:80　　D=135.2.1.1:80

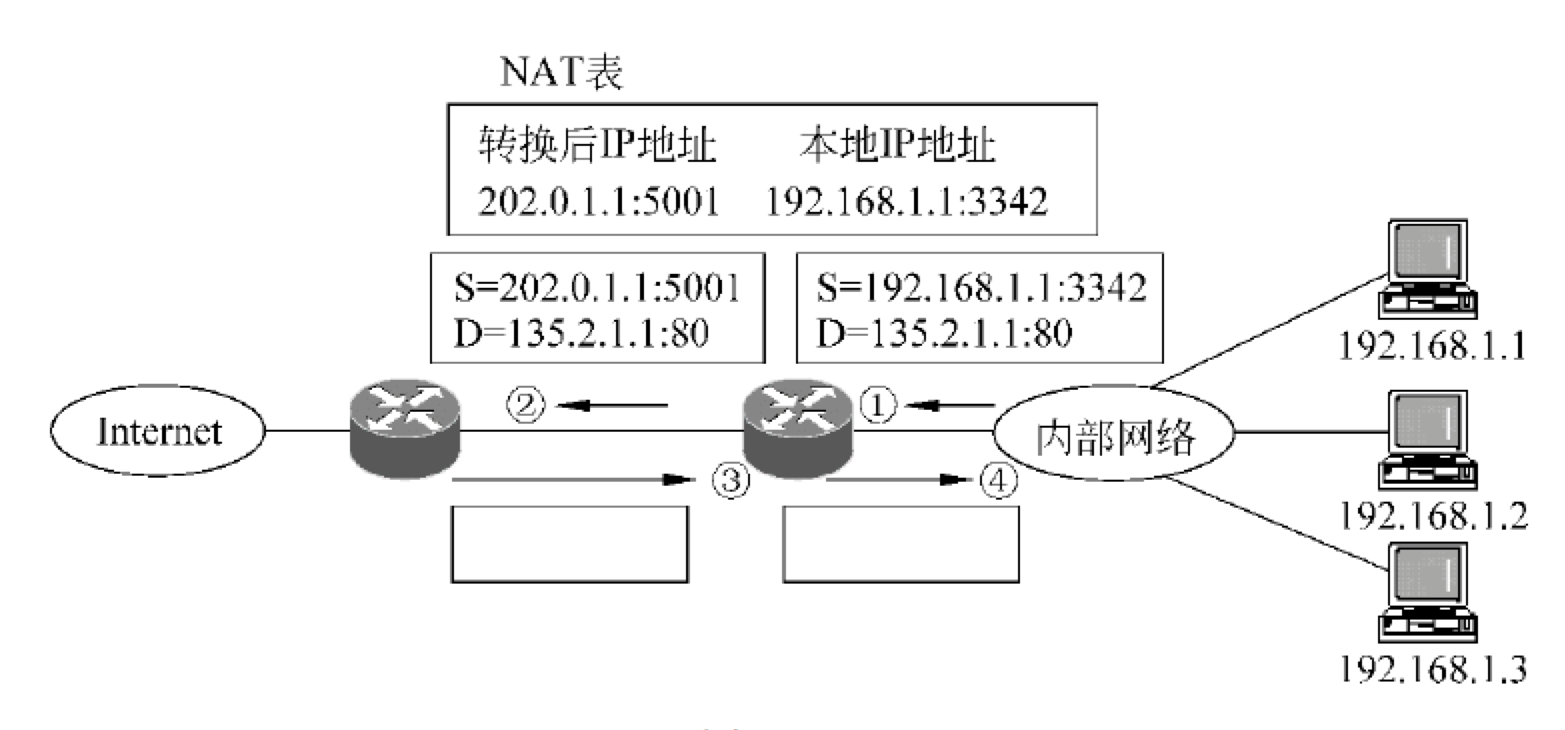


图　13.5

(18) 下述________设备是实施终端接入控制的最佳设备。

A. 交换机　　B. 路由器　　C. 防火墙　　D. 总线

(19) 下述________攻击无法窃取传输过程中的数据。

A. DHCP 欺骗攻击　　B. ARP 欺骗攻击

C. 转发表溢出攻击　　D. 源 IP 地址欺骗攻击

(20) 下述________是防止源 IP 地址欺骗攻击的有效手段。

A. 绑定 MAC 地址和 IP 地址　　B. 绑定接入端口和 MAC 地址

C. 绑定接入端口和 IP 地址　　D. 防火墙设置标准过滤器

二、填空题(本大题共 20 空,每空 1 分,共 20 分)

(1) ________、________和________是三种分别通过攻击主机系统达到破坏信息的可用性、保密性和完整性目的的攻击行为,其中,________破坏信息的可用性,________破坏信息的保密性,________破坏信息的完整性。

(2)________ 、________和________是三种常见的病毒传播方法。

(3) 数字签名必须具有________、________和________特性,其中,________用于确认由签名者本人做出的承诺,________用于确认对特定信息做出的承诺,________保证第三方能够证明签名与签名者之间的关联。

(4) 加密解密算法根据加密密钥和解密密钥是否相同可以分为________和________,________由于加密密钥和解密密钥相同,导致密钥分发比较困难。

(5) 狭义病毒的主要特征是________和________。

三、简答题(本大题共 5 小题,每题 4 分,共 20 分)

1. 简述网络是病毒和蠕虫快速传播通道的理由。
2. 简述 802.1X 实现以太网交换机接入控制的过程。
3. 简述资源访问控制原理及过程。
4. 简述网络设备提供的安全功能的重要性。
5. 简述 NAT 的安全功能。

四、判断题(本大题共 10 小题,每小题 1 分,共 10 分)

(1) 对称密钥算法的密钥分发很困难。

(2) 只要操作系统存在漏洞,主机系统就无法避免远程入侵。

(3) 木马不可能具备狭义病毒特征。

(4) 木马不可能具备蠕虫特征。

(5) 网络安全技术能够解决病毒传播问题。

(6) 操作系统和应用程序漏洞是可以消除的。

(7) 黑客攻击过程和正常访问过程是有所区别的,只是这种区别不是黑白那样分明。

(8) 通过证书和数字签名实现身份鉴别无需鉴别者存储任何有关用户的私密信息。

(9) WEP 和 WPA-PSK 要求所有终端和 AP 配置相同的密钥。

(10) WPA-PSK 下,获取 PMK 即可破译经过无线局域网传输的所有密文。

五、综合题(本大题共 3 小题,每小题 10 分,共 30 分)

1. 网络结构如图 13.6 所示。回答下列问题。

① 给出黑客终端 1 通过 DHCP 欺骗攻击截获终端 A 发送给 Web 服务器的 IP 分组的过程。

② 给出黑客终端 2 通过路由项欺骗攻击截获终端 A 发送给 Web 服务器的 IP 分组的过程。

③ 给出黑客终端 3 通过 ARP 欺骗攻击截获终端 A 发送给 Web 服务器的 IP 分组的过程。

④ 给出防止上述欺骗攻击的方法。

2. 网络结构如图 13.7 所示。回答下列问题。

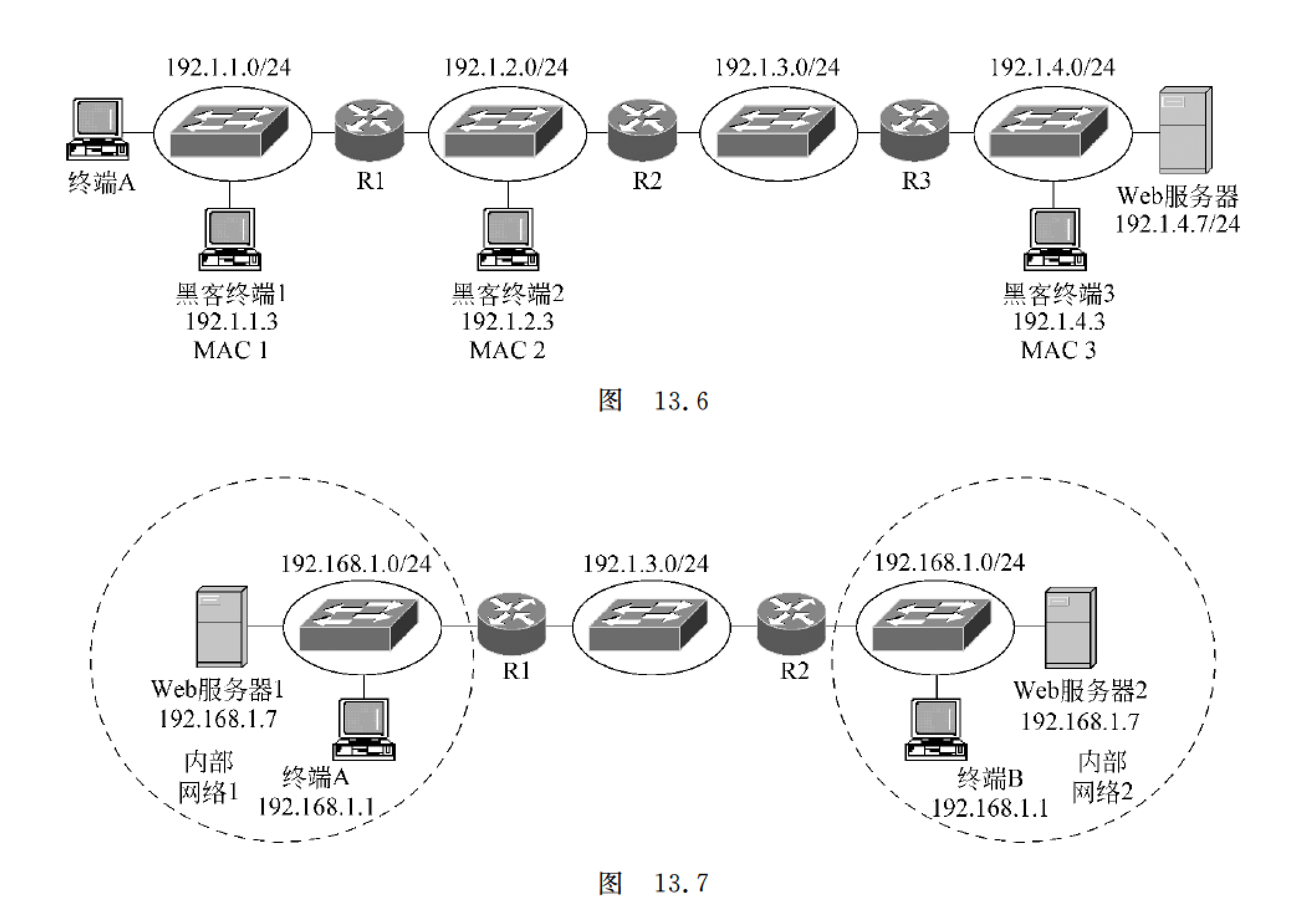


图 13.6

图 13.7

① 给出通过 NAT 技术实现终端 A 访问 Web 服务器 2 和终端 B 访问 Web 服务器 1 所需要的基本配置。

② 采用什么技术可以实现内部网络 1 和内部网络 2 之间的自由通信？图 13.7 需要修改什么配置？给出实现内部网络 1 和内部网络 2 之间自由通信所需要的基本配置。

3. 网络结构如图 13.8 所示。要求实现只允许终端 A 发起访问 Web 服务器，终端 C 发起访问 FTP 服务器，禁止其他一切网络间通信的数据传输控制。

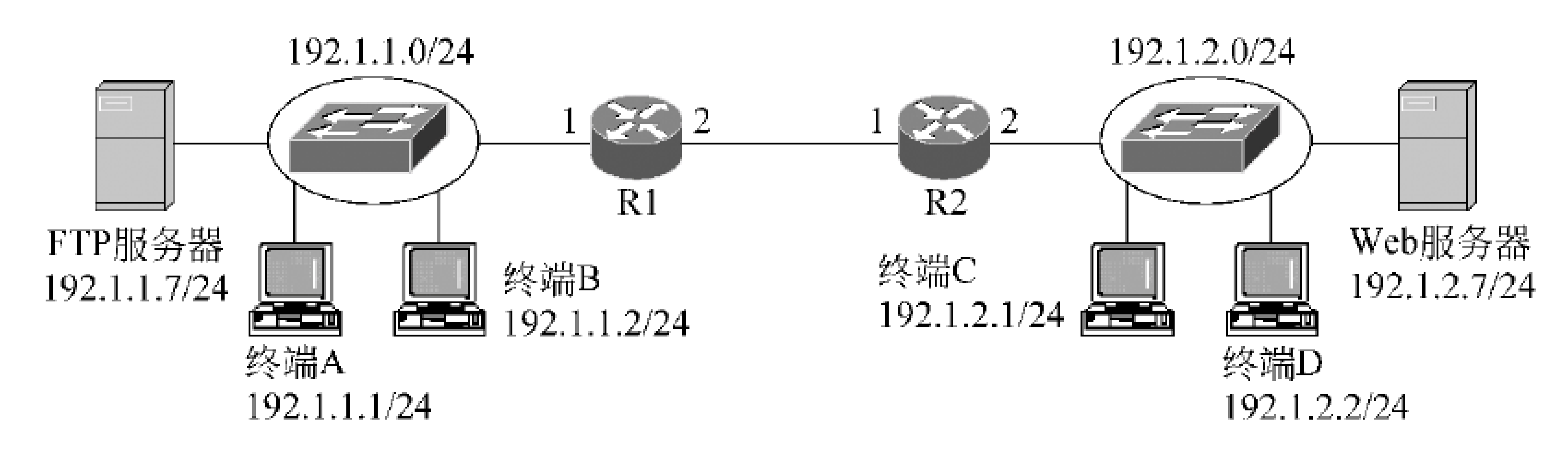


图 13.8

13.2.2 答案

一、选择题答案

1. D	2. C	3. D	4. D	5. B	6. A	7. C	8. A	9. D
10. A	11. D	12. D	13. A	14. D	15. D	16. D	17. B	18. A
19. D	20. C							

二、填空题答案

1. SYN 泛洪攻击,木马,篡改 Web 主页,SYN 泛洪攻击,木马,篡改 Web 主页。
2. 利用邮件传播,浏览嵌入病毒的主页,利用主机系统漏洞上传病毒。
3. 唯一性,关联性,可证明性,唯一性,关联性,可证明性。
4. 对称加密算法,不对称加密算法,对称加密算法。
5. 嵌入宿主程序的一段代码,具有自我复制能力。

三、简答题答案

1. **回答:**目前常见的病毒和蠕虫传播方式有:通过移动存储媒介在主机系统之间相互复制文件、浏览封装恶意移动代码的 Web 主页、打开作为邮件附件的感染病毒的宿主程序、下载并运行感染病毒的实用程序、在共享目录中保存感染病毒的宿主程序、利用主机系统漏洞上传蠕虫或感染病毒的宿主程序。除了通过移动存储媒介传播病毒外,其他传播方式都需通过网络进行,因此网络是病毒和蠕虫快速传播的主要通道。

2. **回答:**①鉴别者或者鉴别服务器配置授权用户标识信息。②用户提供标识信息,如果用户提供的标识信息与某个授权用户的标识信息相同,用户身份得到确认。③将身份鉴别过程中用户向鉴别者传输鉴别信息的 MAC 帧的源 MAC 地址作为源端鉴别的依据,所有源 MAC 地址为该 MAC 地址的 MAC 帧确定为该授权用户发送的 MAC 帧。

3. **回答:**①配置授权用户标识信息。②为每一个授权用户分配资源访问权限。③一旦用户提出资源访问请求,首先鉴别该用户身份,鉴别用户身份的过程就是确定该用户提供的标识信息是否和配置的某个授权用户的标识信息相同的过程。④确定用户提出的资源访问请求是否符合用户匹配的授权用户的资源访问权限。⑤在确定该用户为授权用户且具有资源访问请求中要求的资源访问权限后,完成资源访问过程。

4. **回答:**一是最好由直接连接终端的设备,如交换机实现接入控制,这样才能完全将非法终端隔离在网络外面。二是有些攻击行为只能依靠网络设备予以防止,如防止 DHCP 欺骗攻击需要网络设备禁止伪造的 DHCP 服务器向网络发送 DHCP 响应报文。三是信息截获攻击通常需要改变数据传输路径,网络设备的安全功能能够确保建立并维持的端到端传输路径是正确的。四是容错网络结构能够增强网络的可用性,而网络的可用性是保证信息可用性的基础。五是一切数据必须经过网络设备才能实现传输过程,因此网络设备是对经过网络传输的数据实施检测、监控的理想之处。

5. **回答:**一是由于分配私有 IP 地址的内部网络对于外部网络是透明的,因此连接在外部网络上的黑客终端无法对内部网络终端发起主动攻击。二是在建立内部网络私有 IP 地址和全球 IP 地址之间映射前,外部网络终端无法主动和内部网络终端通信,因此蠕虫病毒很难自动地从外部网络传播到内部网络。三是由于需要通过标准过滤器指定允许进行地址转换的内部网络私有 IP 地址范围,因此内部网络终端无法通过伪造的不存在的内部网路地址去访问外部网络服务器,从而无法对外部网络服务器实施 SYN 泛洪攻击。

四、判断题答案

1. 对　2. 错　3. 错　4. 错　5. 错　6. 错　7. 对　8. 对　9. 对　10. 错

五、综合题答案

1. **回答**：① 在终端 A 连接的以太网中连接一个伪造的 DHCP 服务器，将默认网关地址设置为黑客终端 1 的 IP 地址 192.1.1.3。

② 黑客终端 2 发送源 IP 地址为 192.1.2.3 的路由消息，路由消息中包含用于表明直接和网络 192.1.4.0 连接的路由项<192.1.4.0/24,1>。

③ 黑客终端 3 向路由器 R3 发送一个将 IP 地址 192.1.4.7 和 MAC 地址 MAC 3 绑定的 ARP 报文。

④ 通过为交换机配置信任端口，拒绝伪造的 DHCP 服务器接入以太网；通过实现路由消息源端鉴别和完整性检测，防止路由器接收并处理伪造的路由消息；通过在交换机中绑定 IP 地址和对应的 MAC 地址，防止 ARP 欺骗发生。

2. **回答**：① 路由器 R1 给出用于实现将终端 A 本地 IP 地址转换成全球 IP 地址的全球 IP 地址池，给出将 Web 服务器 1 本地 IP 地址和某个全球 IP 地址绑定的静态映射。路由器 R2 给出用于实现将终端 B 本地 IP 地址转换成全球 IP 地址的全球 IP 地址池，给出将 Web 服务器 2 本地 IP 地址和某个全球 IP 地址绑定的静态映射。路由器 R1 和 R2 中必须配置静态路由项，通过这些静态路由项将以这些全球 IP 地址为目的地址的 IP 分组准确路由给下一跳。

② 采用 VPN 技术，内部网络 1 和内部网络 2 必须使用不同网络地址的本地 IP 地址，建立路由器 R1 和 R2 之间的隧道，为隧道接口分配本地 IP 地址。

3. **回答**：路由器各个接口配置的分组过滤器如表 13.2 所示。

表　13.2

协议	源 IP 地址	源端口号	目的 IP 地址	目的端口号	动作
路由器 R1 接口 1 输入方向					
TCP	192.1.1.1/32	any	192.1.2.7/32	80	正常转发
TCP	192.1.1.7/32	20	192.1.2.1/32	any	正常转发
TCP	192.1.1.7/32	21	192.1.2.1/32	any	正常转发
IP	any		any		丢弃
路由器 R1 接口 1 输出方向					
TCP	192.1.2.1/32	any	192.1.1.7/32	20	正常转发
TCP	192.1.2.1/32	any	192.1.1.7/32	21	正常转发
TCP	192.1.2.7/32	80	192.1.1.1/32	any	正常转发
IP	any		any		丢弃
路由器 R2 接口 2 输入方向					
TCP	192.1.2.1/32	any	192.1.1.7/32	20	正常转发
TCP	192.1.2.1/32	any	192.1.1.7/32	21	正常转发
TCP	192.1.2.7/32	80	192.1.1.1/32	any	正常转发
IP	any		any		丢弃

续表

协议	源 IP 地址	源端口号	目的 IP 地址	目的端口号	动作
路由器 R2 接口 2 输出方向					
TCP	192.1.1.7/32	20	192.1.2.1/32	any	正常转发
TCP	192.1.1.7/32	21	192.1.2.1/32	any	正常转发
TCP	192.1.1.1/32	any	192.1.2.7/32	80	正常转发
IP	any		any		丢弃

13.3 试 卷 三

13.3.1 试卷

一、选择题(本大题共 20 小题,每小题 1 分,共 20 分)

(1) 下述________和信息保密性无关。

A. 加密解密算法　B. 终端接入控制　C. 病毒　D. 拒绝服务攻击

(2) 下述________和阻止信息嗅探攻击无关。

A. 交换机端口静态配置为全双工通信方式

B. 鉴别 DNS 资源记录

C. 交换机端口之间禁止镜像

D. 用交换机取代集线器

(3) 下述________表示黑客们编写的、具有自动传播和自动激活特性的完整程序。

A. 恶意代码　B. 病毒　C. 木马　D. 蠕虫

(4) ________可以证明数据发送端、保障数据的完整性及防止重放攻击。

A. AH　B. ESP　C. TLS　D. SET

(5) 下述________不是 DNS Sec 的功能。

A. 源端鉴别　B. 完整性检测

C. 加密资源记录　D. 域名与 IP 地址绑定关系验证

(6) 下述________是 SNMP 有别于 Telnet 的地方。

A. 配置网络设备　B. 查询网络设备状态

C. 单台终端在线配置多个网络设备　D. 网络设备主动报告发生的事件

(7) 对于入侵防御系统,下述________的描述是错误的。

A. 一般的入侵防御系统和杀毒软件一样,需要定时更新攻击特征库

B. 正常访问过程和入侵过程存在差异,但无法严格区分

C. 规则是长期观察信息流变化过程后得出的一些规律性的总结

D. 入侵防御系统能够检测出没有发作的病毒

(8) 下述________描述是错误的。

A. 攻击特征检测机制容易漏报

B. 异常检测机制容易误报
C. 协议译码能够检测出恶意错误
D. 攻击特征检测机制能够检测出未知攻击

(9) 关于入侵防御系统功能,下述________的描述是错误的。
A. 防御病毒发作引发的攻击行为　　B. 防御对资源的非法访问
C. 防御分布式拒绝服务攻击　　D. 防御信息嗅探和截获攻击

(10) 对于防火墙,下述________的描述是错误的。
A. 防火墙主要用于控制网络之间的数据交换过程
B. 防火墙能有效抑制内网终端中的木马外泄信息
C. 防火墙能减缓拒绝服务攻击
D. 防火墙能杜绝病毒从一个网络传播到另一个网络

(11) 对于无状态分组过滤器,下述________的描述是错误的。
A. 能够控制两个不同网络之间的数据传输过程
B. 能够控制两个终端之间的数据传输过程
C. 能够控制两个进程之间的数据传输过程
D. 能够控制一次完整应用所涉及的数据交换过程

(12) 下述________不是专用网络的特点。
A. 使用本地 IP 地址　　B. 不和其他网络共享传输路径
C. 不能和其他网络相互通信　　D. 使用 TCP/IP 协议栈

(13) 下述________是专用网络和虚拟专用网络的本质区别。
A. 使用本地 IP 地址
B. 实现数据内部网络子网间安全传输
C. 使用公共网络提供的数据传输通路
D. 使用 TCP/IP 协议栈

(14) 下述________不是隧道的功能。
A. 实现内部网络各个子网间互连
B. 实现连接在 Internet 上的终端远程接入内部网络
C. 两个 IPv6 网络通过 IPv4 网络实现互连
D. 实现内部网络终端和公共网络终端之间的通信

(15) 下述________不是 IP Sec 提供的功能。
A. 实现使用本地 IP 地址的 IP 分组经过 Internet 传输
B. 实现数据经过 Internet 的安全传输
C. 实现数据的源端鉴别
D. 实现源端和目的端之间的相互身份鉴别

(16) 关于 WEP,下述________描述是错误的。
A. 用循环冗余码检测数据完整性
B. 伪随机数生成算法作为产生一次性密钥的单向函数
C. 采用流密码体制
D. 一次性密钥不会重复

(17) 关于 WEP 加密，下述________描述是错误的。

A. 终端和 AP 必须具有相同密钥 K

B. 为了同步一次性密钥，发送端需要向接收端发送 IV 明文

C. 黑客无法通过嗅探经过无线网络传输的信息获得密钥 K

D. 黑客无法破译嗅探到的经过无线网络传输的密文

(18) 下述________描述是正确的。

A. 获取 WEP 密钥能够破译一切经过无线局域网传输的密文

B. 获取 WPA-PSK 密钥能够破译一切经过无线局域网传输的密文

C. 获取 WPA 用户标识信息能够破译一切经过无线局域网传输的密文

D. 一旦和 AP 成功建立关联，便能够破译一切经过无线局域网传输的密文

(19) 下述有关 802.1X 的描述________是错误的。

A. 802.1X 是基于用户的接入控制技术

B. 802.1X 和访问控制列表结合才能精细控制终端接入

C. 终端多次接入某个交换机端口只需一次身份鉴别过程

D. 身份鉴别过程中记录授权用户使用的终端的 MAC 地址

(20) NAT 对防止下述________攻击是无效的。

A. 连接在公共网络上的黑客发起的对内部网络终端的主动攻击

B. 因为下载包含病毒的网页而感染病毒

C. 内部网络终端发起的对外部网络中的服务器的 SYN 泛洪攻击

D. 从外部网络传播蠕虫到内部网络

二、填空题(本大题共 20 空，每空 1 分，共 20 分)

(1) ________、________和________是三种分别通过攻击通信系统达到破坏信息的可用性、保密性和完整性目的的攻击行为。其中，________破坏信息的可用性，________破坏信息的保密性，________破坏信息的完整性。

(2) 目前常见的基于网络的防病毒措施包括________、________、________和________。其中，________的作用是隐藏内部网络，使外部网络终端无法发现内部网络中的终端，________的作用是通过控制内部网络和外部网络之间的信息交换过程隔断病毒向内部网络传播的通路，________的作用是通过监控流经关键链路的信息流发现病毒并隔断病毒传播通路，________的作用是通过管制疑似与病毒传播有关的信息流的流量来抑制病毒传播。

(3) 入侵防御系统分为________和________。

(4) 入侵防御系统工作过程分为________、________、________和________。

三、简答题(本大题共 5 小题，每题 4 分，共 20 分)

1. 简述 Telnet 和 SNMP 管理网络设备的方式。
2. 简述网络入侵防御系统和防火墙的区别。
3. 简述隧道和 IP Sec 是实现 VPN 的基础的理由。
4. 简述 WEP 的缺陷。
5. 简述接入控制设备的作用。

四、判断题(本大题共 10 小题,每小题 1 分,共 10 分)

(1) 任何两个不同报文的报文摘要肯定不同。

(2) 安装病毒查杀软件是应对病毒感染和传播的唯一方法。

(3) PGP 是一个具有数字签名和加密功能的软件,可以用于实现邮件的安全传输。

(4) 入侵防御系统可以代替防火墙。

(5) 入侵检测系统的干预行为往往滞后攻击行为。

(6) 分组过滤器可以正常转发或丢弃两个特定终端之间传输的分组。

(7) 分组过滤器可以正常转发或丢弃两个特定用户之间传输的分组。

(8) VPN 中内部网络各个子网的 IP 地址空间是相互独立的,允许两个不同子网分配相同的本地 IP 地址空间。

(9) VPN 中连接在不同内部网络子网的终端可以通过本地 IP 地址实现相互通信。

(10) WPA-PSK 下,每一个终端和 AP 有着独立的 TK。

五、综合题(本大题共 3 小题,每小题 10 分,共 30 分)

1. 网络结构如图 13.9 所示。回答下列问题。

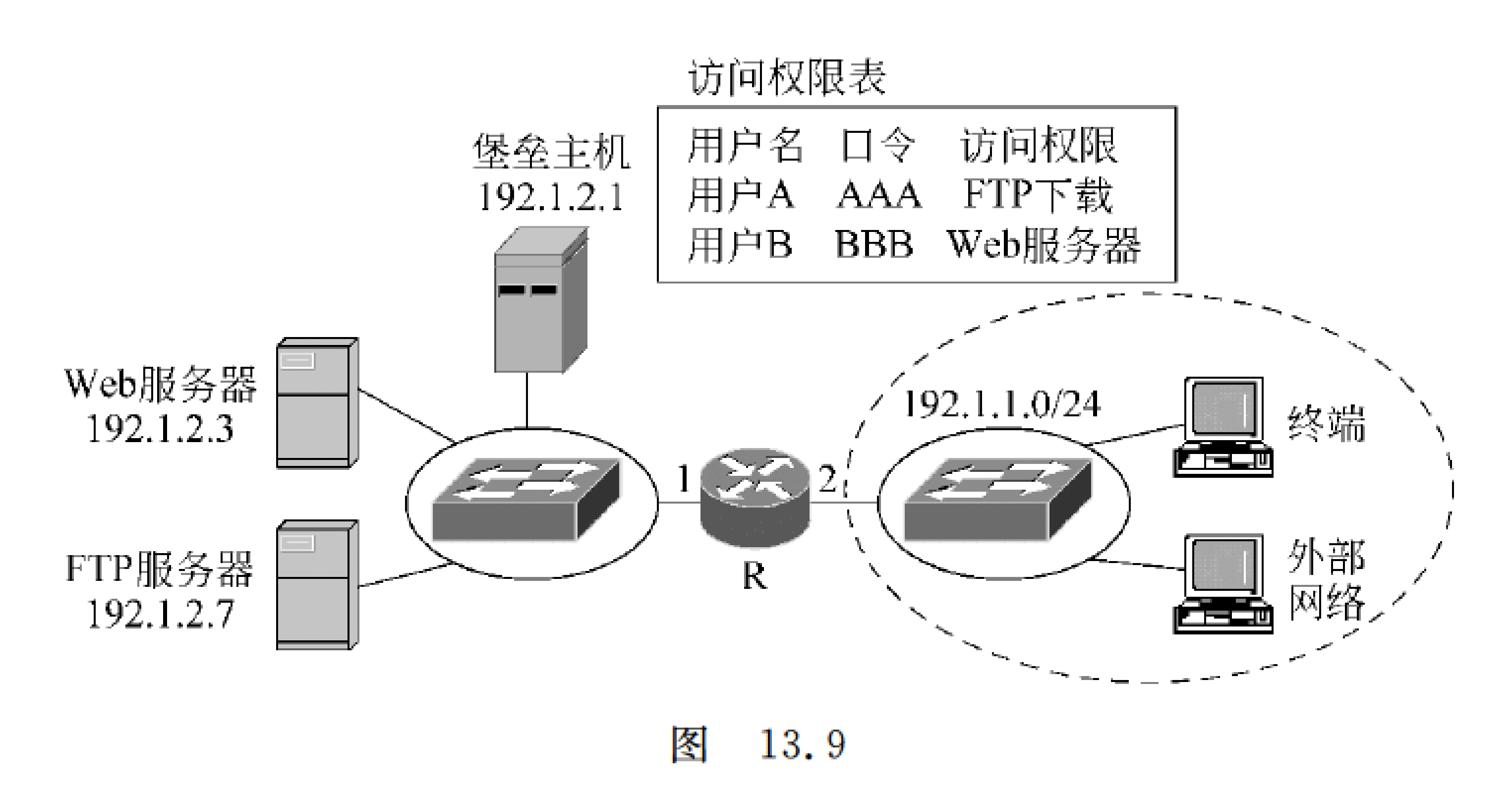
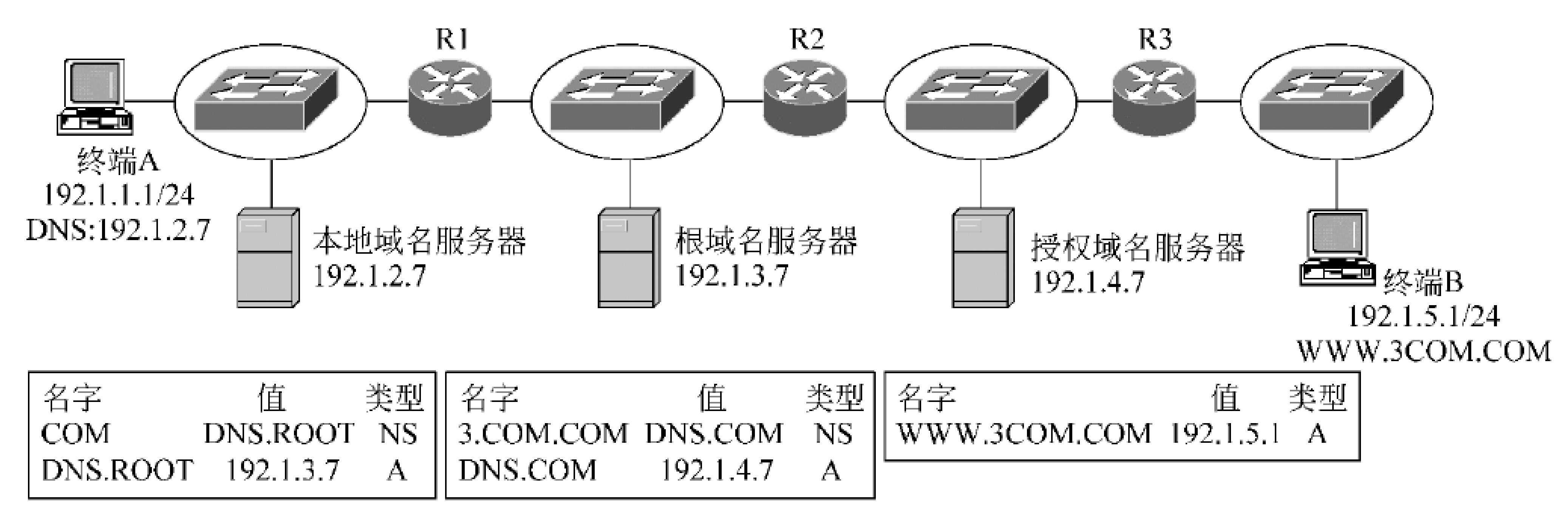


图　13.9

① 访问控制策略要求外部网络终端必须通过堡垒主机访问内部网络服务器,给出路由器 R 实现这一访问控制策略需要配置的无状态分组过滤器。

② 根据图中给出的访问权限表,描述用户 A 访问 FTP 服务器过程。

2. 网络结构如图 13.10 所示。域名解析采用递归方式,给出 DNS Sec 配置,并简述资源记录源端鉴别和完整性检测过程。



名字	值	类型
COM	DNS.ROOT	NS
DNS.ROOT	192.1.3.7	A

名字	值	类型
3.COM.COM	DNS.COM	NS
DNS.COM	192.1.4.7	A

名字	值	类型
WWW.3COM.COM	192.1.5.1	A

图　13.10

3．网络结构如图 13.11 所示。回答下列问题。

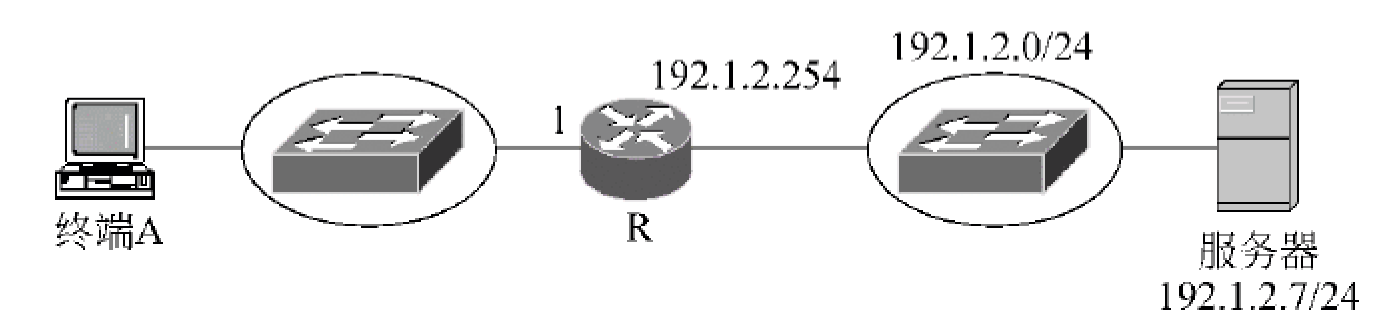


图 13.11

① 假定终端 A 通过 PPPoE 接入网络，给出路由器 R 必要配置，并简述终端 A 访问服务器过程。

② 假定终端 A 通过 802.1X 接入网络，给出路由器 R 必要配置，并简述终端 A 访问服务器过程。

③ 简述这两种接入方式的本质区别。

13.3.2 答案

一、选择题答案

1．D　2．B　3．D　4．A　5．C　6．D　7．D　8．D　9．D
10．D　11．D　12．D　13．C　14．D　15．A　16．D　17．D　18．A
19．C　20．B

二、填空题答案

1．Smurf 攻击，信息嗅探攻击，篡改信息攻击，Smurf 攻击，信息嗅探攻击，篡改信息攻击。

2．NAT，防火墙，网络入侵防御系统，流量管制，NAT，防火墙，网络入侵防御系统，流量管制。

3．主机入侵防御系统，网络入侵防御系统。

4．收集信息，检测入侵行为，反制入侵行为，登记和分析。

三、简答题答案

1．**回答**：Telnet 远程登录网络设备后，可以通过终端输入所有网络设备支持的命令。SNMP 可以通过 SET 命令对被管对象设置新值，但要求一是被管对象必须是该网络设备 MIB 包含的被管对象，二是该被管对象必须是可读写的。

2．**回答**：一是检测的信息不同，防火墙只检测网络间传输的信息，入侵防御系统能够检测流经任何网段的信息。二是检测机制不同，防火墙根据配置的访问控制策略确定信息是否违反安全策略，并丢弃违反安全策略的信息，入侵防御系统根据建立的攻击特征库和描述正常访问过程的行为模式确定是否是攻击信息，并对攻击信息予以反制。三是作用不同，防火墙的作用是通过静态配置访问控制策略来限制网络间允许交换的信息流类型，入侵防御系统通过分析已经发现的入侵行为，如蠕虫传播过程、木马窃取信息资源过程和黑客利用操作系统漏洞实施的攻击过程，提取出攻击特征，通过对这些攻击特征的匹配操作，可以检测出正在进行的攻击行为，并予以反制，因此入侵防御系统主要作用是阻止已知的和未知的攻击行为继续。四是入侵防御系统通过在多个关键结点和关键链路

收集信息,并对这些信息的检测结果进行综合分析来发现分布式拒绝服务攻击和其他对网络的侦察行为,防火墙不具有这一功能。

3. **回答**:隧道是一种通过公共网络传输任意格式分组的技术,它将任意格式分组封装后作为以隧道两端 IP 地址为源和目的 IP 地址的外层 IP 分组的净荷,在完成外层 IP 分组隧道两端之间传输的同时,实现任意格式分组隧道一端至隧道另一端的传输过程。IP Sec 能够实现 IP 分组净荷隧道两端之间的安全传输。隧道与 IP Sec 结合可以实现任意格式分组公共网络任意两个端点之间的安全传输。这恰恰是 VPN 的设计目标,用公共网络实现内部网络各个子网之间互连,同时又能保证内部网络封装形式的数据各个子网间的安全传输。

4. **回答**:一是由于密钥有效期间,所有终端共享 2^{24} 个一次性密钥,因此很容易通过建立一次性密钥字典破译密文。二是一旦黑客获得密钥,即可破译经过无线局域网传输的所有密文。三是身份鉴别机制容易被黑客破解。四是完整性检测机制无法检测出精心设计的篡改。

5. **回答**:接入控制设备的作用:一是作为普通路由器实现接入网络与 Internet 的互连。二是实现对用户终端的接入控制,主要功能包括鉴别接入用户身份、动态分配 IP 地址、建立用于指明通往用户终端的传输路径的路由项。

四、判断题答案

1. 错　2. 错　3. 对　4. 错　5. 对　6. 对　7. 错　8. 错　9. 对　10. 对

五、综合题答案

1. **回答**:① 路由器接口配置的无状态分组过滤器如表 13.3 所示。

表　13.3

协议	源 IP 地址	目的 IP 地址	动作
路由器 R 接口 1 输入方向			
IP	192.1.2.1/32	192.1.1.0/24	正常转发
IP	any	any	丢弃
路由器 R 接口 1 输出方向			
IP	192.1.1.0/24	192.1.2.1/32	正常转发
IP	any	any	丢弃

② 用户 A 首先通过外部网络中的任何一个终端访问堡垒主机,在堡垒主机弹出的身份鉴别界面中输入用户名:用户 A,口令:AAA。然后在堡垒主机弹出的资源地址栏中输入“ftp://192.1.2.7”。允许正常下载 FTP 服务器中文件,但如果向 FTP 服务器上传文件,会出现警告:无上传权限。

2. **回答**:域名解析过程如图 13.12 所示,根域名服务器需要验证授权域名服务器发送的用于指明域名 WWW.3COM.COM 和 IP 地址 192.1.5.1 之间绑定关系的资源记录。授权域名服务器用自己的私钥 S3COM 对资源记录数字签名,同时给出自己的公钥 P3COM。根域名服务器首先通过自己保存的资源记录<.3COM .COM SHA-1

(P3COM)＞验证授权域名服务器的公钥 P3COM，然后用授权域名服务器的公钥 P3COM 验证授权域名服务器的数字签名，并完成资源记录＜ WWW. 3COM. COM 192. 1. 5. 1＞的完整性检测。根域名服务器同样用自己的私钥 SR 对资源记录＜ WWW. 3COM. COM 192. 1. 5. 1＞数字签名，由于根域名服务器的公钥 PR 通过有公信力的媒体公告，因此本地域名服务器和终端 A 无须验证根域名服务器公钥 PR，直接用公钥 PR 验证根域名服务器的数字签名，并完成资源记录＜ WWW. 3COM. COM 192. 1. 5. 1＞的完整性检测。

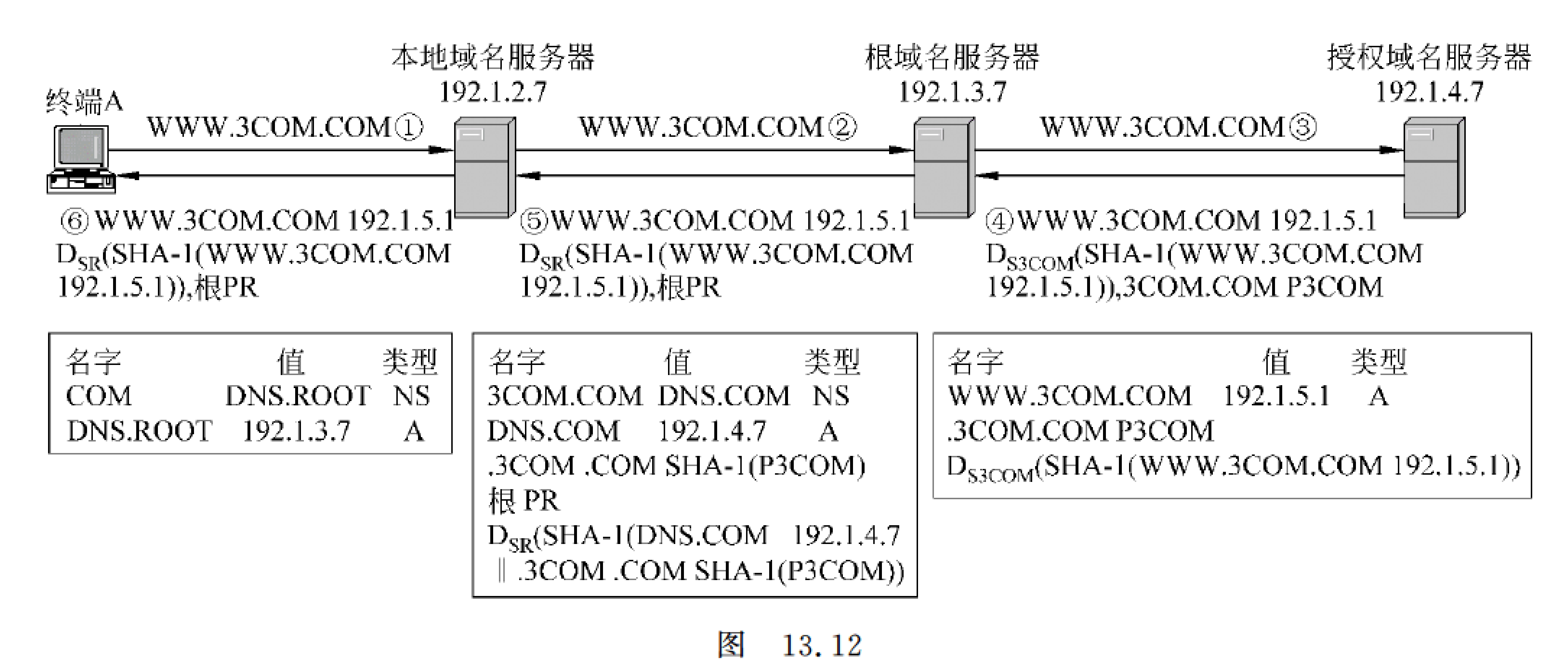


图 13.12

3. **回答**：① 路由器 R 配置注册用户列表和 IP 地址池，终端 A 用户启动 PPPoE 连接程序，PPPoE 连接程序首先建立终端 A 与路由器 R 之间的 PPP 会话，基于 PPP 会话建立 PPP 链路，由路由器 R 完成对用户的身份鉴别，为终端 A 分配一个地址池中没有分配的 IP 地址，在路由表中增添一项将分配给终端 A 的 IP 地址与终端 A 和路由器 R 之间的 PPP 会话绑定的路由项。

② 路由器 R 配置注册用户列表，终端 A 用户启动 802. 1X 客户程序，由路由器 R 完成对用户的身份鉴别，并将终端 A 的 MAC 地址记录在路由器 R 接口 1 的访问控制列表中，然后为终端 A 配置网络信息，配置网络信息后的终端 A 像连接在以太网上的普通终端一样访问网络。

③ PPPoE 建立终端 A 和路由器 R 之间基于以太网的等同于点对点链路的 PPP 会话，然后由路由器 R 通过 PPP 完成接入用户的身份鉴别、IP 地址分配和在路由表中添加将分配给终端 A 的 IP 地址与终端 A 和路由器 R 之间的 PPP 会话绑定的路由项等功能。完成这些步骤后，终端 A 可以对网络实施访问。

路由器 R 通过 802. 1X 完成接入用户的身份鉴别后，只是允许正常转发通过接口 1 接收的、源 MAC 地址为终端 A 的 MAC 地址的 MAC 帧，终端 A 必须像连接在以太网上的普通终端一样完成网络信息配置后，才能对网络实施访问。

参考文献

[1] 沈鑫剡等. 计算机网络学习辅导与实验指南. 北京：清华大学出版社，2011.
[2] 沈鑫剡等. 计算机网络技术及应用学习辅导和实验指南. 北京：清华大学出版社，2011.
[3] 沈鑫剡. 计算机网络安全. 北京：清华大学出版社，2009.
[4] 沈鑫剡. 计算机网络. 第 2 版. 北京：清华大学出版社，2010.
[5] 沈鑫剡等. 计算机网络技术及应用. 第 2 版. 北京：清华大学出版社，2010.
[6] 沈鑫剡等. 计算机网络技术及应用. 北京：清华大学出版社，2007.
[7] 沈鑫剡. 计算机网络. 北京：清华大学出版社，2008.
[8] 沈鑫剡等. 多媒体传输网络与 VOIP 系统设计. 北京：人民邮电出版社，2005.
[9] 沈鑫剡等. IP 交换网原理、技术及实现. 北京：人民邮电出版社，2003.
[10] 沈鑫剡. 广域网原理、技术及实现. 北京：人民邮电出版社，2000.
[11] 沈鑫剡. 交换式以太网原理、技术及实现. 北京：人民邮电出版社，1999.
[12] James Trulove 著. 沈鑫剡译. 局域网布线. 北京：人民邮电出版社，2002.